Exchange 2000 Conferencing Server

Concepts and Planning Guide

© Copyright Microsoft Corporation, 1999-2000. All Rights Reserved

Note: This documentation is an early release of the final product documentation. It is meant to accompany software that is still in development. Some of the information in this documentation may be inaccurate or may not be an accurate representation of the functionality of the final retail product. Microsoft assumes no

responsibility for any damages that might occur either directly or indirectly from these inaccuracies.

DRAFT

Introduction 8
Benefits of Exchange Conferencing Server 9
Coordinating Conference Invitations 9
Finding a Conference Host 9
Creating the Conference Topology 10
Providing Security and Encryption Features 10
Conferencing Across a Firewall 10
Controlling System and Network Resources 10
Using Exchange Conferencing Server in Your Organization 11
Scheduling a Conference 11
Scheduling Conference Resources 11
Reserving a Conference Resource 11
Inviting a Conference Resource 11
Joining a Conference 12
Key Components 14
Conference Management Service 14
Data Conferencing Provider 15
How Data Conferencing Provider Works 15
Multipoint Control Unit 16
Video Conferencing Provider 17
How Video Conferencing Provider Works 17
MADCAP 18
Auxiliary Components 18
Outlook Calendar 18
Conference Window 19
Conference Calendar Mailbox 20
Conference Access Pages 20
Architecture 20
Internal Components and Services 21
Conference Management Service 21
Data Conferencing Provider 22
Video Conferencing Provider 22
Conference Access Pages 22
Exchange T.120 Multipoint Control Unit 22

DRAFT

Exchange H.323 Video Conference Bridge 22
Third-Party Providers (Optional) 22
Additional Components and Services 22
Exchange 2000 Server 22
Windows 2000 MADCAP Service 23
Windows 2000 Certificate Services 23
Windows 2000 Active Directory 23
Microsoft Management Console 23
Windows Client 23
Internet Browser 23
E-mail Client 23
T.120 Client 24
TAPI Telephony Libraries 24
Security **24**
Controlling Access to Conferences 24
Public Conferences 24
Public Conferences With Password 24
Private Conferences 25
Client Certificates Required for Private Conferences 25
Security Supplied by the Conference Technology Provider 25
Accessing the Conference Location URL 26
Administration **26**
Windows Site-Based Service 26
Administrative Groups 27
Conference Technology Provider Service Management 27
Logging Reports 27
Planning Overview **28**
System and Software Requirements **28**
Server Requirements 28
Client Requirements 29
Conference Organizers 29
Data Conferencing Client 29
Video Conferencing Client 30

DRAFT

Hardware Requirements **30**
Servers 30
Client Computers 31
Data Conferencing Client 31
Video Conferencing Client 31
Video Conference Performance 32
Permissions **33**
Managing Exchange Conferencing Server 33
Exchange Conferencing Server Services 33
Resource Management 33
Conference Management Service **35**
Single Conferencing Site 35
Multiple Conferencing Sites 36
Conference Technology Provider Location 37
Conference Access Pages 37
Default Conference Access Pages 38
Scalability 39
Conference Calendar Mailbox 39
Conference Resources 39
When is a resource busy 40
Naming Conventions 41
Reliability Planning 41
Backup and Restore 42
Best Practices **42**
Data Conferencing Provider Planning **43**
Windows 2000 Site Architecture 43
Working with Remote Data Conferencing Sites 44
Network Considerations 44
Conference Participants Location 44
Conferencing Across a Firewall 45
Secure Conferencing 46
Reliability Planning 46
Scalability and Performance 46
Multipoint Control Unit 47

DRAFT

Multipoint Control Unit Security 47
Network Deployment 48
Backbone Topology 48
Hub and Spoke Topology 48
Decentralized Topology 49
MCU Connections and Types 50
Video Conferencing Provider 52
Multicast Basics 52
IP Multicast 52
Multicast Address 53
Time-to-Live Value 53
Multicast Group 53
Multicast Scope 54
Reserved Addresses 54
DHCP and MADCAP Configuration 55
Multiple MADCAP Servers 55
Network Configuration 55
Routers 56
Bridging Video Conferences 56
Resources 57
Best Practices 58
Installing Exchange Conferencing Server 59
Before the Installation 59
Plan Your Deployment 59
Verify Requirements for Installation 59
System Requirements 59
Hardware Requirements 60
Installation 60
Conferencing Server Components 60
Initial Installation 61
Subsequent Installation 62
Post-Installation Tasks 62
Server 62
Client 62

DRAFT

DRAFT

CHAPTER 1

Welcome to Exchange 2000 Conferencing Server

Introduction

Microsoft Exchange 2000 Conferencing Server provides an extensible platform for real-time online conferencing. You can schedule and conduct online conferences with live audio and video, and you can offer additional features such as whiteboard notes, chat, application sharing, and file transfer. You can structure online conferences by reserving conference resources, inviting conference participants, and setting the properties for each conference. Conferences can be public or private and can accommodate two or more attendees. The centralized reservation system of Exchange Conferencing Server allows you to schedule and join conferences from the Outlook calendar. If you are not an Outlook user, you can join conferences from a Web browser, using the conference location URL included in the conference request message.

Exchange Conferencing Server provides powerful tools for real-time collaboration between coworkers in large and small companies. The primary components of Exchange Conferencing Server are Conference Management Service, Data Conferencing Provider, and Video Conferencing Provider. Data Conferencing Provider, which is based on T.120 protocols, and Video Conferencing Provider, which is based on IP multicast protocols, are called conference technology providers. Third-party conference technology providers are also available.

Conference Management Service Conference Management Service is an extensible platform that you can use with Microsoft and third-party conferencing technologies. Conference Management Service coordinates and manages conferencing technologies and resources, and tracks and controls access to conferences.

Data Conferencing Provider Data Conferencing Provider is a conferencing technology that provides multiple collaboration tools, including multiparty application sharing, chat, whiteboard notes, and file transfer. These features are based on the T.120 International Telecommunications Union–Telecommunication Standardization Sector (ITU-T) Recommendation for Multimedia Conferencing. Data Conferencing Provider creates a data conferencing environment that optimizes conference performance and network resources, and provides a bridge for participants on remote sites and across firewalls.

Video Conferencing Provider Video Conferencing Provider is a conferencing technology that provides multiparty video and audio conferences over multicast-enabled IP networks. Video Conferencing Provider allows conference participants to see and hear each other simultaneously, eliminating the need for a parallel teleconference. The multicast-enabled network optimizes network bandwidth, while distributing audio and video communications to conference participants.

Exchange Conferencing Server integrates the features of all installed conference technology providers and provides these features to conference participants; for example, if you install a third-party telephone conference provider along with Data Conferencing Provider, you can schedule a conference using a resource that has both data and telephone capabilities. Conference participants can share desktop applications and communicate by telephone at the same time. Together, Video Conferencing Provider and Data Conferencing Provider can provide a bridge to a Video Conferencing Provider multicast conference for Microsoft NetMeeting clients that use the H.323 unicast audio/video standard.

Chapter 2 describes each of these components in detail.

Benefits of Exchange Conferencing Server

Online conferencing applications were once difficult to use. Exchange Conferencing Server offers the following improvements over previous online conferencing technologies:

- Coordinates conference invitations
- Finds a conference host
- Creates the conference topology
- Provides security and encryption features
- Enables conferencing across a firewall
- Controls the use of network and system resources

Coordinating Conference Invitations

In the past, to schedule and participate in a conference, the conference organizer and participants had to enter specific information about the conference; for example, which Internet Locator Service (ILS) server to use, the name of the participant server to call, whether someone would be using Microsoft NetMeeting to invite them, or whether they would have to call someone to access the conference. Typically, this information was different for each participant.

Today, Exchange Conferencing Server is integrated into Microsoft Outlook 2000 calendaring and includes all information necessary to connect each participant to the conference. Conference organizers and participants do not need information about the servers or underlying technologies the conference uses.

Finding a Conference Host

There are two models for conferencing: peer-to-peer, such as NetMeeting, and client-server, such as Lotus SameTime. Before Exchange Conferencing Server, conferencing applications required the organizer and all participants to know and work with the selected connection type.

In peer-to-peer conferencing, conference participants interconnect to establish direct links between their desktops. One or more desktops serve as hosts of the conference. The conference host must be available for the duration of the conference. If the top-node host leaves, the conference ends.

In client-server conferencing, conference participants interconnect through a central server. If the server is unavailable at the scheduled conference time, the organizer must schedule a new conference on another server. At the time of a conference, Exchange Conferencing Server selects a load-balanced, best-connected server for the conference. This eliminates the problem of server unavailability.

Creating the Conference Topology

In the past, you had to understand conference topologies to host successful conferences. This included understanding how networks deliver data and how to minimize the number of data copies sent over the network, or it could mean hosting the conference in more than one location and interconnecting the groups of participants.

In contrast, Exchange Conferencing Server creates the optimal data conference topology for you by building the topology according to the network location of the client at the time the client joins the conference.

Providing Security and Encryption Features

Even if you use Exchange Conferencing Server within a secured intranet, you may want to ensure that only invited people can access the information discussed in the online conference. When scheduling an online conference from Outlook 2000, you can choose one of three levels of security: public, public with password, and private. Also, Conference Management Service can require that users authenticate themselves prior to accessing the conference. For further information on these types of conferences, see Security in Chapter 2.

Conferencing Across a Firewall

To meet with people online, you must share a common network. The Internet is frequently used for this. While you want to share information with others, you also want to prevent unauthorized access to your company's resources. Firewalls prevent unauthorized access but they also prevent the flow of information in online conferences.

With Exchange Conferencing Server, you can host secure online conferences with attendees outside your organization. Also, Exchange Conferencing Server is designed to make each conference attendee’s participation seamless, regardless of the attendee’s location on the Internet.

Controlling System and Network Resources

Most companies have a limited number of meeting rooms. Typically, meetings in these rooms are scheduled ahead of time, so the organizer knows that the room is reserved. While online conferences do not require a physical location, they do place demands on the company's network and server infrastructure.

The cost of a virtual meeting depends on the type of online conference you are hosting. An online telephone conference uses different resources than an online video conference. Exchange Conferencing Server bases its resource model on the status of the conference technology providers and their scheduled resources. Through the Exchange Conferencing Server resource model, you can define and manage the conferencing infrastructure to support the demands of online conferences within your organization. For more information on configuring resources, see Resources in Chapter 4.

Using Exchange Conferencing Server in Your Organization

Exchange Conferencing Server allows members of widely dispersed teams to meet online, removing geographical barriers and improving productivity in the process. Online conferences can build team interaction and encourage collaboration across great distances. Team members with specialized knowledge can participate in conferences on the other side of the country or on the other side of the world, without the expense and time required to travel to a physical location.

Exchange Conferencing Server can help you approximate the experience of a formal face-to-face meeting. Instead of finding and reserving an available meeting room, you invite a conference resource—a virtual meeting room.

Scheduling a Conference

You schedule a conference by creating a meeting request and inviting a conference resource. If the associated conference technology providers accept the conference request, Conference Management Service stores the conference details in the conference calendar mailbox. This persistent representation of the online conference gives conference technology providers a storage location for information associated with the conference, such as an archive for a recording of the conference. Conference Management Service maintains the accuracy of the conference definition by processing all conference updates and publishing the associated free and busy data.

Scheduling Conference Resources

You can schedule a conference resource in two ways. You can reserve a resource or you can invite a resource.

Reserving a Conference Resource

You can directly reserve a conference resource using Outlook 2000. Outlook 2000 checks the free and busy data for the resource and adds the resource to the invitation if the resource is available. This gives you a confirmed reservation. When you send an invitation, the conference resource is reserved and the URL for the conference is included in the invitations.

You can restrict who can reserve conference resources by applying permissions to the conference resource calendar in Outlook. Log on to Outlook using the conference resource user account. In the Inbox, right-click **Calendar**, and then click **Properties**. On the **Permissions** tab, grant or deny users permissions to schedule conference resources.

Inviting a Conference Resource

If you are not using Outlook 2000, you can still schedule conferences and reserve conference resources, but you must use an application that can send a meeting request. You can use the following applications:

- Previous versions of Outlook
- Outlook 2000 in offline mode

- Exchange 5.0 client
- Outlook Web Access

Using one of these applications, e-mail an invitation to the conference resource. If the resource is available, the application sends you an e-mail acknowledgement, accepts the reservation, and provides the conference URL. This is called asynchronously reserving a resource.

To restrict who can asynchronously reserve conference resources:

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **Active Directory Users and Computers**.
2. In Active Directory Users and Computers, from the **View** menu, click **Advanced Features**.
3. Double-click **System**, and then double-click **Exchange Conferencing**.
4. In the details pane, select the mailbox you want, right-click, and then click **Properties**.
5. Click the **Exchange General** tab, and then click **Delivery Restrictions**.
6. Apply delivery restrictions.

Joining a Conference

In a typical online conference, the user asks to attend by going to the location the conference URL specifies. Every online conference is identified by a conference access URL. All conference participants use the same URL regardless of the combination of conference technology providers the conference is using. A user can access the URL of an online conference before, during, or after the scheduled start time.

Conference Management Service receives the user’s request and attempts to find the associated conference in the conference calendar mailbox. After Conference Management Service locates the conference definition in the conference calendar mailbox, it determines whether a password or user authentication is required. Conference Management Service then works in conjunction with the conference technology providers to obtain the correct information for the user.

While participants are in conference, Conference Management Service permits the organizer to modify the end-time and properties of the conference.

When a participant joins a video conference, a script runs on the client computer that investigates whether client configuration and network connectivity characteristics allow a direct connection to a multicast conference. If any of the prerequisites are not met, Conference Management Service attempts to connect the participant to the conference over an H.323 unicast connection. You can disable this feature for each resource individually.

When a multicast connection is established, users can see a video of all participants, including any participants using an H.323 unicast connection, and they can hear up to five active speakers simultaneously.

When an H.323 unicast connection is established, users can hear up to five speakers, but they can see only the current speaker.

Note H.323 bridging is available only for conferences using both Video Conferencing Provider and Data Conferencing Provider. The actual H.323/multicast bridging is accomplished over Data Conferencing Provider multipoint control unit (MCU) servers. The bridge is installed as a part of a T.120 MCU component installation.

DRAFT

Exchange Conferencing Server Concepts

Key Components

As a companion product to Microsoft Exchange 2000 Server, Exchange 2000 Conferencing Server enables remote, real-time collaboration between team members of large and small companies. Exchange Conferencing Server consists of three interrelated, key components: Conference Management Service, Data Conferencing Provider, and Video Conferencing Provider. Together, these components create an extensible environment for online collaboration.

Conference Management Service

Conference Management Service manages conference resources and supports conference technology providers. Conference Management Service provides access to online conferences through a Web site hosted by Microsoft Internet Information Services (IIS). You can configure these Web pages to require user authentication, thus limiting access to private conferences.

Conference resources are mailbox-enabled objects in Microsoft Windows 2000 Active Directory. Conference Management Service publishes the availability of conference resources through Exchange 2000 Server free and busy data. Microsoft Outlook uses this information to indicate the availability of conference resources at specific times.

When you schedule a conference, Conference Management Service inserts a URL for the conference into the conference invitation. Conference attendees then use this URL to access the conference through conference access pages. Conference Management Service stores all scheduled conferences in a specific mailbox, which is called the conference calendar mailbox. This information is used to create a persistent representation of the conference format, structure, and any additional information associated with the conference. Conference Management Service also makes it possible for e-mail clients that cannot reserve conference resources to invite conference resources.

Conference Management Service controls the lifetime of an online conference. This service works in cooperation with each conference technology provider to ensure that the conference starts and ends according to the schedule.

Using the conference resources it defines, Conference Management Service keeps a list of all scheduled conferences. Public conferences are included in a list of available meetings on the conference access pages, and any Web client can participate in a public conference. Private conferences are not listed; to join a private conference, participants must have the correct URL.

Conference Management Service allows the Exchange Conferencing Server administrator to analyze schedule and conference data available in audit log files. These formatted, comma-delimited files are created daily and are available on the conferencing server hosting the active instance of Conference Management Service.

Data Conferencing Provider

Data Conferencing Provider is a conference technology provider that enables conference participants to share applications, conduct whiteboard sessions, transfer documents, and chat. This data collaboration is accomplished using tools such as Microsoft NetMeeting or other applications that support the T.120 network communications standard. Participants experience data conferencing in varying ways, depending on their T.120 and Internet browser applications.

How Data Conferencing Provider Works

Data Conferencing Provider creates a resource scheme based on its maximum permissible number of simultaneous conference participant connections. This maximum participation count is the physical resource against which the conferencing resource makes reservations when you invite the resource to an online conference. Each conferencing resource has a size associated with it, and Conference Management Service considers this size the cost of hosting the conference. Data Conferencing Provider subtracts the resource cost from the maximum participation count. If the remaining available maximum participation count is greater than the resource cost, the resource is reserved for the time period you request. If the available count reaches zero for any specific requested time, Data Conferencing Provider prompts Conference Management Service to publish a busy indication, and no additional reservations are accepted.

During a data conference, the computer of each participant is connected to a T.120 multipoint control unit (MCU). On the conferencing site, you can install the T.120 MCU on multiple servers running Microsoft Windows 2000, and then you can group them into clustered farms of servers. These farms of MCUs provide the platforms on which each scheduled data conference is hosted. When a participant joins a data conference, Data Conferencing Provider uses the following criteria to selects the best MCU:

- Which MCUs are available and in service?
- Is the conference already running on an MCU?
- What load do existing conferences place on the MCU?
- Are there any administratively defined restrictions on which MCU can be used?
- What is the network location of the participant?
- Is the participant inside the local conferencing site?
- Is the participant closer to another conferencing site?
- Is the participant outside the organization's network?

Using these criteria, Data Conferencing Provider connects a conference participant to a load-balanced MCU that is closest to his or her network location, limiting the number of data copies sent between these locations. Because Data Conferencing Provider assigns an MCU when a participant joins a conference, the interconnection of the remaining MCUs is always dynamic and can optimize server availability and users’ network locations.

If the client is running NetMeeting 3.01 or later, Data Conferencing Provider places the controls for NetMeeting within the conference window’s browser frame. Both Microsoft Internet Explorer 4.01 and NetMeeting 3.01 or later are required to join a private

conference that uses a public certificate for authentication and encryption of the conference data.

You can install the T.120 multipoint control unit independently of other services. Each MCU automatically attempts to retrieve a machine certificate from Windows 2000 Certificate Services. The MCU hosts private conferences by authenticating the connection between the MCU and clients when building the conference topology. Without a valid certificate, the MCU cannot host a private data conference.

A data conference has the following features:

Application sharing You can share a program running on one computer with other participants in the conference. Participants can review the same data and see the actions as the person sharing the application works on the program; for example, editing content or scrolling through data. Participants can share Windows-based applications without any special knowledge of the application. The person sharing the application can choose to collaborate with conference participants, allowing them to take turns editing or controlling the application. Only the person sharing the program must have the application installed on his or her computer.

Also, with NetMeeting 3.0, you can share your desktop, allowing another person to remotely control your computer.

Shared clipboard You can share data with other participants using cut, copy, and paste operations; for example, you can copy information from a local document and paste the contents into a shared application. The shared clipboard provides an easy way for participants to exchange data between shared and local applications.

File transfer You can send a file in the background to one or more conference participants using a file transfer. Because the file transfer occurs in the background, participants can continue sharing an application or using other data conferencing features.

Whiteboard You can load or sketch diagrams and organizational charts, or display other graphic information in this multi-page, multi-user drawing application. Whiteboard is object-oriented (versus pixel-oriented), allowing you to move and manipulate the contents using a click and drag operation. In addition, you can use a remote pointer or highlighting tool to point out specific content or sections of shared pages.

Chat You can type text messages to share common ideas or topics with conference participants, or you can use text messages to record conference notes and action items. You can also use chat to communicate if audio is not available. The NetMeeting *whisper* feature allows you to have a separate, private conversation with one of the conference participants during a group chat session.

NetMeeting 3.01 or later is the recommended client software for Data Conferencing Provider. It provides the features mentioned previously; can run as an embedded control on the Web page; and facilitates private, secure conferences.

Multipoint Control Unit

Multipoint control units (MCUs) are required for data conferences. MCUs interconnect multiple conference participants, and synchronize and distribute conference data between participants.

The NetMeeting client includes an MCU. Each client connection to an MCU requires a separate copy of the conference data. This means that in a peer-to-peer conference, a NetMeeting application with ten participants sends ten copies of the information. If the participant is on a modem or at the other end of a slow WAN link, the response can be slow.

To prevent clients from sending multiple copies of the conference data, move the MCU to a central server and enable each participant to connect to it. If you deploy this MCU server so that it bridges multiple networks, a conference can take place between participants on your intranet and participants on the Internet. Also, when the conference is hosted on a server, the organizer is not required to remain in the conference until it ends. In peer-to-peer conferencing, the organizer's computer acts as an MCU and must stay in the conference for its duration.

This single server deployment does not address the issue of multiple participants on the remote end of a WAN link, because the deployment still requires multiple copies of the conference data to be transmitted across the link. In this scenario, you should place an MCU at both ends of the WAN link and instruct participants to connect to the MCU closest to their physical locations on the network. Although this increases the complexity of participation in a conference, you can build a conference topology in this manner using peer-to-peer logic only. But if you stretch the conference over multiple WAN links, and if multiple participants often travel, changing which MCU is closest, this manual solution becomes impossible to manage. Data Conferencing Provider offers a solution to these problems by creating an automatic topology that sends single instances of data across the WAN link. A persistent location for the conference allows participants to come and go. Data Conferencing Provider automatically directs a client to the closest server, and in addition, provides a high level of security.

Video Conferencing Provider

Video conferencing is a technology that allows two or more people in remote locations to exchange voice and video images in real time. NetMeeting offers limited video conferencing capabilities; for example, with NetMeeting 3.01, you can establish a peer-to-peer video conference using the International Telecommunications Union–Telecommunication Standardization Sector (ITU-T) H.323 unicast standard.

Video Conferencing Provider allows users to organize and participate in multiparty video and audio conferences. Video Conferencing Provider technology is based on the Internet Engineering Task Force (IETF) IP multicast standards. In addition, Video Conferencing Provider conferences are available for clients with H.323 capabilities, such as NetMeeting, over an IP multicast/H.323 unicast bridge—which is part of Exchange Conferencing Server and can be deployed on a separate MCU server. Video Conferencing Provider combines greater efficiency on multicast-enabled networks with wider accessibility and low-bandwidth support over non-multicast networks, such as the Internet.

How Video Conferencing Provider Works

When a conference with a Video Conferencing Provider resource begins, a special multicast IP address is requested from a Multicast Address Dynamic Client Allocation Protocol (MADCAP) server and reserved for the conference. MADCAP, which is part of the Windows 2000 Dynamic Host Configuration Protocol (DHCP) service, assigns a multicast group IP address to each Exchange video conference. This multicast IP address cannot be

used in subsequent reservations until the initial reservation expires. The expiration time is defined as the scheduled conference end time plus the maximum video conference extension time. You configure the maximum video conference extension time from the Video Conferencing Provider in XXXXXXPlaceholderXXXXXXXXXXX. The maximum video conference extension time is the maximum amount of time, in minutes, that the conference organizer can extend a conference in progress.

When you join a Video Conferencing Provider conference as a multicast client, your multicast client Microsoft ActiveX control receives the multicast IP address that the Video Conferencing Provider reserved for the conference. The control then *subscribes* to the multicast conference and retrieves and sends video and audio data to and from that multicast address.

In a pure multicast video conference, no servers participate in the actual transfer of video and audio traffic. If routers are in the way of the multicast packets, they serve as replicators or multiplexers, forwarding packets to the network segments on which the clients participating in the conference are located.

MADCAP

MADCAP servers must exist on the network and routers must be multicast-aware for a multicast video conference to work. Servers running Windows 2000 DHCP can assign multicast and unicast addresses. You configure multicast scopes and corresponding multicast IP ranges with Windows 2000 Administrative Tools. This is required before users can successfully schedule and conduct video conferences. Once you set and activate these scopes, Windows 2000 DHCP service can provide multicast addresses in the same way it normally provides unicast IP addresses.

If a participant cannot connect directly to the multicast streams and Data Conferencing Provider is installed on the site, Video Conferencing Provider requests that Data Conferencing Provider supply a bridge between the multicast streams and the participant.

Auxiliary Components

This section describes the auxiliary components that support the key components of Exchange Conferencing Server: Outlook calendar, conference window, conference calendar mailbox, and conference access pages.

Outlook Calendar

You can schedule online conferences using Outlook 2000.

To schedule an online conference:

7. On an Outlook meeting request, click This is an online meeting.
8. In the list, click Microsoft Exchange Conferencing.
9. reserve a conference resource for the meeting as follows:
    - In **Show Names from the**, select **All Conference Resources**.
    - Locate the resource you want in the list that appears; for example, *ParisVideoConf(5)* can accommodate a five-person video conference on the Paris stie.

- Click **Resources**, and then click **OK**.

10. Make your remaining meeting selections.

You must invite a conference resource for the meeting. This is the virtual meeting room in which the conference is held. Outlook 2000 reserves the conference resource before sending prospective attendees conference invitations.

A link (URL) to the online conference is included in the invitations that conference participants receive. To join the conference, attendees can access this link with a browser. Outlook 2000 users receive a conference reminder for the online conference that includes a **Join Conference** option, which users can click to join the conference. You can also join a conference by right-clicking the meeting request in your Outlook calendar.

Online conference organizers who cannot book online conferences directly using Outlook 2000 can use previous versions of Outlook or Outlook Web Access. Using these applications, you can invite the conference resource as a conference attendee. You cannot, however, identify the conference as private using these applications, as with Outlook 2000. Thus, uninvited attendees can join the conference. In addition, the conference location, or URL link, is not automatically included in the initial conference invitation. Instead, you must forward the URL to all conference attendees. This URL is included in the conference accept message from Conference Management Service.

Conference Window

When you join a conference, your browser displays a conference window. The conference window is customized for each participant according to the conference technology providers used and whether participants access the conference before, during, or after the scheduled time of the conference. The left frame of the conference window, the conference panel, displays general information about the conference. The conference window includes one or more additional frames, each of which is associated with a specific conference technology provider. The set of conference technologies available in a conference is defined by the conference resource the organizer selects when scheduling the conference.

The conference panel includes:

- The conference schedule and amount of time remaining in the conference.
- A mail-enabled link to the conference organizer.
- The subject of the conference.
- Information about whether the conference is private (attendance is restricted to the invitees).

Additionally, the following links to other Web pages (depending on configuration) are available for the conference organizer:

- Request to extend the length of the conference in session.
- Request to change the resource on which the conference is hosted. This is usually done to allow additional participants to join the conference.

The conference window displays a warning to participants five minutes before the end of the conference. At the end of the five-minute period participants are disconnected from conference resources, unless the conference organizer configures a grace period and the

conference technology providers honor it. Grace periods allow attendees to arrive early or leave late. You can set grace periods that apply to all scheduled conferences.

Conference Calendar Mailbox

Each conferencing site requires a conference calendar mailbox assigned to Conference Management Service. You must assign the mailbox before a conference organizer can schedule an online conference using conference resources.

For performance reasons, you should place the conference calendar mailbox on an Exchange server that is as close as possible to the conferencing server hosting Conference Management Service—or preferably on the same server if Exchange and Exchange Conferencing Server are installed on the same server. The conference calendar mailbox stores scheduled online conferences as single entries. Each entry defines the properties of the conference, such as the security level and conference participants. Some conference technology providers also use the conference calendar mailbox to store additional information associated with an online conference; for example, Video Conferencing Provider stores the description of the multicast video conference. A third-party conference archive provider may use the conference calendar mailbox as a storage location for a recording of the conference.

Conference Access Pages

Each conferencing site’s instance of Conference Management Service has a Web site that hosts the conference access pages. All conference participants access these pages, which also include a list of links to public conferences. You can select one of these links to attend the conference.

Because all conference participants must retrieve pages from this Web site, the site's network address must be accessible to all users. If this includes attendees from the Internet, the conference access pages must be available over the Internet as well.

Architecture

Exchange Conferencing Server contains a group of interrelated components and services that work together to provide real-time conferencing. In addition to these internal features, external components and services from other products are necessary for Exchange Conferencing Server to work. This section discusses these internal and external components and services and the recommended client configuration.

The following figure illustrates how these components and services relate to one another. A description of each component follows.

DRAFT

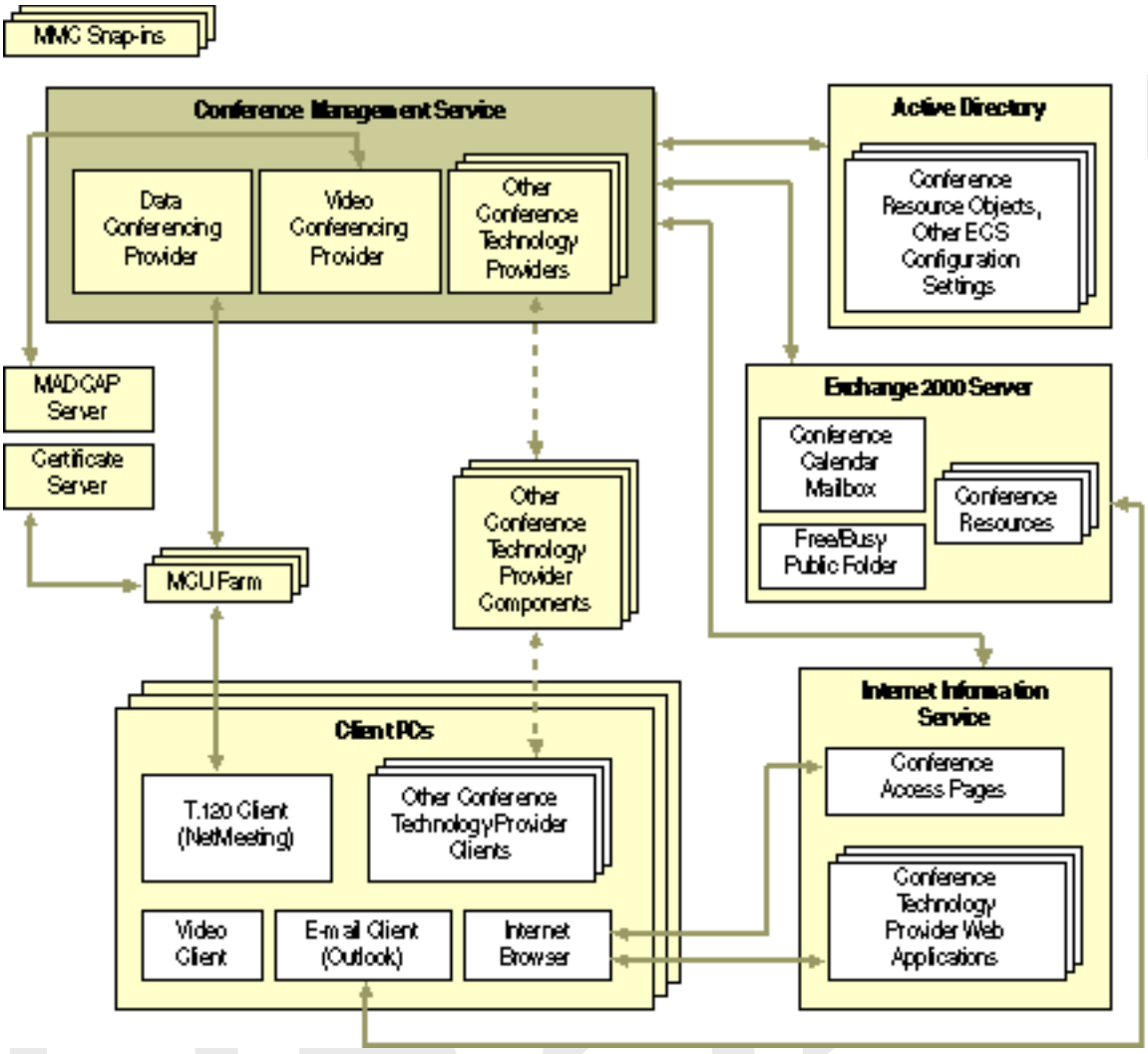

Figure 2.1 Exchange 2000 Conferencing Server interrelated components and services

Internal Components and Services

The following components and services are included with Exchange 2000 Conferencing Server:

Conference Management Service

Conference Management Service manages conference technology providers and allows for the management of conference resources, scheduled conference profiles, conference duration, and verification of attendee access rights. Conference Management Service controls the client's access to all online conferences. Clients access conference access pages from a Web site hosted by IIS.

Data Conferencing Provider

Data Conferencing Provider is a conference technology provider consisting of a controller —which must be installed on the same server as Conference Management Service—and one or more T.120 MCUs. You can install MCUs on a separate server that does not have other Exchange Conferencing Server or Exchange components.

Video Conferencing Provider

Video Conferencing Provider is always installed with Conference Management Service. In addition, a Windows 2000 MADCAP server must exist on the network for video conferencing to function.

Conference Access Pages

Conference participants use these HTML pages to join and participate in conferences. Exchange Conferencing Server uses IIS to host the conference access pages. A portion of the access control for these pages is based on IIS settings for public or private conferences.

Exchange T.120 Multipoint Control Unit

The T.120 MCU service runs as a component of Data Conferencing Provider and is used to interconnect network connections between participants in a data conference. The MCU communicates with the Data Conferencing Provider controller through a Distributed Component Object Model (DCOM) session and with conference participants through the T.120 protocol.

Exchange H.323 Video Conference Bridge

The H.323 video conference bridge service runs as a component of the T.120 MCU. It permits clients with NetMeeting that are unable to directly connect to Video Conferencing Provider multicast conferences to connect through a H.323 unicast session.

Third-Party Providers (Optional)

In addition to the two conference technology providers that Exchange Conferencing Server includes, Conference Management Service can accommodate third-party conference technology providers that are specifically designed for it.

Additional Components and Services

The following are additional components and services that are required for Exchange Conferencing Server. These are required components and services that must be present on your Windows 2000 site or on your client’s computers for Exchange Conferencing Server to work.

Exchange 2000 Server

Exchange Conferencing Server uses Exchange 2000 Server to store the conference schedule and reserve conference resources. This makes it easy to apply Exchange policies to elements of Exchange Conferencing Server.

Exchange Conferencing Server uses two types of Exchange mailboxes: a conference calendar mailbox and a conference resource mailbox. The conference calendar mailbox

stores the definitions and structure of all conferences. The conference resource mailbox is invited to a conference to reserve the virtual conference room of the conference technology providers hosting the conference.

Windows 2000 MADCAP Service

MADCAP servers must exist on the network and routers must be multicast-aware for multicast video conferences to work. Servers running Windows 2000 DHCP can assign multicast and unicast addresses. You configure multicast scopes and corresponding multicast IP ranges with Windows 2000 Administrative Tools. This is required before users can successfully schedule and conduct video conferences.

Windows 2000 Certificate Services

The T.120 MCU uses Windows 2000 Certificate Services to enroll in the X509v3 public certificate authentication. The MCU uses these certificates to authenticate conference participants and connections with other MCUs during secure conferences.

Conference participants can obtain client certificates from Windows 2000 Certificate Services. To join private conferences, participants using NetMeeting 3.01 must have client certificates.

Windows 2000 Active Directory

Exchange Conferencing Server stores all configuration information within Active Directory. This facilitates multimaster, remote, and offline administration. Exchange Conferencing Server also uses information in Active Directory to access the network topology.

Microsoft Management Console

Exchange Conferencing Server and conference technology providers use Microsoft Management Console (MMC) for system administration.

Windows Client

Clients running Windows 2000 can participate in multicast video conferences because Windows 2000 is multicast-enabled. Exchange Conferencing Server uses the services of Windows 2000 Server.

Internet Browser

Internet Explorer 4.01 or higher is recommended, but a browser that supports frames and can download ActiveX controls will also work. Conference participants use an Internet browser to participate in conferences through conference access pages.

E-mail Client

Conference organizers use an e-mail client to schedule conferences and reserve conference resources. Outlook 2000 is the preferred e-mail client for Exchange Conferencing Server. You can also use previous versions of Outlook or Outlook Web Access.

T.120 Client

NetMeeting 3.01 is the preferred T.120 client. This application allows conference participants to connect to an MCU and send and receive data during a data conference. You can also use other T.120-compliant applications.

TAPI Telephony Libraries

Windows 2000 includes Telephony Application Programming Interface (TAPI) 3.0 telephony libraries. These libraries support multicast video conferencing.

The best client experience for conferencing comes from the integration of Outlook 2000, Internet Explorer 4.01 or later, NetMeeting 3.01, and the TAPI 3.0 telephony libraries for multicast video conferencing.

Security

Exchange Conferencing Server provides security when:

- Controlling access to conferences
- Accessing conferences
- Participating in a conference

Because the hosting conference technology provider sets the guidelines for participation in an online conference, the conference technology provider also sets the format for conference security. Conference Management Service controls security for creating and accessing conferences, so this type of security is the same for all conference technology providers.

Controlling Access to Conferences

When you schedule a conference, you control access to it by specifying whether the conference is public or private. With Exchange Conferencing Server, you can create public conferences, public conferences that require a password, or private conferences.

Public Conferences

Public conferences are accessible to any user who has access to the URL. By default, conferences are public.

When you schedule an online conference using Outlook Web Access for Exchange 5.5 or versions of Outlook earlier than Outlook 2000, you can schedule only public conferences that are not password protected. All public conferences are listed on a page accessible from the home page of the conference access page. The URL for the list of public conferences is http://<*server_name*>/conferencing/list.asp, where *server_name* is the name of the MCU hosting the conference.

Public Conferences With Password

You can create a public conference that participants can access with the correct password. The conference technology provider uses the password to further limit access. To create a public conference with a password, verify that the **Allow external attendees** check box is selected and include the password on the conference invitation.

Private Conferences

You can create a private conference so that only attendees that you invite can participate. The conference technology provider (or Conference Management Service) checks the credentials of each participant to see if he or she is authorized to participate in the conference. If Conference Management Service performs the check, it uses IIS to check the user's credentials. Only attendees who have credentials known to IIS can access the conference pages. To create a private conference, verify that the **Allow external attendees** check box is cleared on the conference invitation.

The type of conference, whether it is public, public with password, or private, is also communicated to the associated conference technology providers. The conference technology provider may provide additional security for private conferences; for example, Data Conferencing Provider forces public certificate authentication and subsequent transmitted data encryption hosting a private conference.

Client Certificates Required for Private Conferences

A digital certificate is an electronic document that grants credentials to the users or computers on the network. Certificates are required for users who want to join private conferences.

Data Conferencing Provider recognizes certificates that are granted from a trusted certificate authority (CA), such as Windows 2000 Certificate Services. Certificate Services must exist in the Active Directory forest of domains. The MCU queries Certificate Services to obtain a machine certificate, which it then uses to authenticate conference attendees. The MCU uses Windows CryptoAPI (CAPI) to scan Active Directory and the local registry for a list of certificate authorities that are valid in the organization. The MCU then compares the client certificates against this list to validate the authenticity of the attendee.

If you want users with third-party certificates to participate in private conferences, verify that your organization subscribes to the third-party certification services and that the trusted certificate authorities hierarchy is properly configured.

Security Supplied by the Conference Technology Provider

Each conference technology provider included in the online conference receives information about the security level of the conference. The level at which the conference technology provider secures the information in the conference varies depending on the conference technology provider.

Data Conferencing Provider allows any user to access a public conference. For password-protected public conferences, users must have a password to access the conference. For a private conference, a public certificate must be exchanged with the MCU that authenticates the user as an attendee of the conference. In addition, the connection between the user and the authenticating MCU (and any other MCU in the conference) is secured using Secure Sockets Layer (SSL) encryption.

Video Conferencing Provider does not distinguish between public and private conferences. Multicast clients can participate in private video conferences, but their connection will not be encrypted. The experience will be similar to participating in a public conference. However, clients without multicast connectivity that connect to the conference through an H.323 unicast connection cannot participate in private video conferences.

Accessing the Conference Location URL

The location of each online conference is defined by a unique URL:

http://<*server*>/<*root*>/<*conference id*>[<*password*>]

Conference Management Service and IIS create the conference access pages that participants use during the conference. Because users access all conferences through IIS virtual roots, you can place global IIS-defined restrictions on conference resources. For example, you can limit participation in the conference to a specific group of users.

Administration

You can administer Exchange Conferencing Server services by using the Exchange Conferencing Services snap-in. You manage each conferencing site within the organization separately. Use a user account with adequate permissions from a computer running Windows 2000 that is a member of the Windows forest for your site. You can also administer these services without Window 2000 by installing Windows Terminal Services.

You can use the same administrative security groups for Exchange Conferencing Server services that you use to manage Exchange.

Windows Site-Based Service

Unlike the server-based services that Exchange 2000 Server provides, in which mailboxes exist on a specific computer, Exchange Conferencing Server is a Windows site-based service. Exchange Conferencing Server is implemented by a number of interrelated services.

Conference Management Service defines the top-level of the Exchange Conferencing Server installation. You install each instance of Conference Management Service on a computer on a Windows 2000 site. Only one instance of Conference Management Service is active on each site. An additional instance of Conference Management Service on a site idles without processing the conferencing load, acting as a backup host server for the conferencing site. The host server you configure defines which server is active; the first instance of Conference Management Service that you install on the site is the default host server.

To administer Exchange Conferencing Server at a specific location:

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **XXXXplaceholderXXXX**.
2. In the console tree, right-click **Exchange Conferencing**.
3. Click **Manage**, and then in the scroll box, select the name of your conferencing site.
4. In the details pane, double-click ***Site Name* Conferencing Site**, where *Site Name* is the name of your conferencing site.

From here, you can administer Conference Management Service, MCUs, conference resources, and conference technology providers.

Administrative Groups

When installing Conference Management Service, you must specify the Exchange administrative group in which to install the service. These groups allow you to assign administrative permissions to specific users who then control different servers or services. When you install Conference Management Service from a specific Windows 2000 site in an administrative group, all instances of Conference Management Service that you install in that site are placed in the same administrative group; therefore, you can always manage the servers on a specific site from a single administrative group.

Conference Technology Provider Service Management

You can control each service installed as part of Exchange Conferencing Server from System Manager or Windows 2000 Services, under Administrative Tools. You can change the state of a service only if you have the associated Windows permissions on that computer.

Logging Reports

Conference Management Service can produce a report log for a number of operations. You can specify the events that you want included in the log.

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **XXXXplaceholderXXXX**.
2. In the console tree, right-click **Exchange Conferencing**.
3. Click **Manage**, and then in the scroll box, select the name of your conferencing site.
4. In the details pane, double-click ***Site Name* Conferencing Site**, where *Site Name* is the name of your conferencing site.
5. Right-click ***Site Name* Conferencing Site**, click **Logging**, and select the events you want to include in the log.

Each event is written to a comma-delimited text file that is named for the date it was generated. These files are automatically purged according to the same schedule you defined for the Exchange 2000 message log files.

You can find these files in the following Exchange logs directory:

\<*servername*>\<*servername*>.ecs

Conference technology providers may also provide event logs that you can find in the same location.

These files allow you to analyze the operation of Exchange Conferencing Server; for instance, if you find that a large number of users are scheduling online conferences against resources on another Windows site, this may be an indicator that you should deploy an additional conferencing site and associated resources closer to the physical location of the users.

CHAPTER 3

Planning Your Exchange Conferencing Server Installation

Planning Overview

Before you install Microsoft Exchange 2000 Conferencing Server, you must review the overall system and component requirements. This chapter discusses some of the global planning issues, such as system requirements, hardware requirements, permissions, and best practices. Chapter 4 discusses specific component planning issues.

System and Software Requirements

There are system and software requirements for servers that host online conferences and computers that participants use during the conferences.

Server Requirements

To run a complete installation of Exchange Conferencing Server, you must have Microsoft Exchange 2000 Server, Microsoft Windows 2000 Server, Microsoft Windows 2000 Multicast Address Dynamic Client Allocation Protocol (MADCAP), Microsoft Windows 2000 Certificate Services, Microsoft Internet Information Services (IIS), and Active Directory available in your organization.

Microsoft Exchange 2000 Server Exchange Conferencing Server requires at least one Exchange server in your organization. You can install Exchange Conferencing Server components on the same server as Exchange or on another computer in your organization.

Microsoft Windows 2000 Server You must install Exchange Conferencing Server on Windows 2000 Server or Windows 2000 Advanced Server, in the same domain as the Exchange server. All conference calendar mailboxes and conference resources for the conference technology providers must have Windows accounts within this domain. Also, at least one Exchange server in the domain must include or have a replica of the free/busy public folder.

Microsoft Windows 2000 MADCAP Services Use MADCAP to configure IP multicast address scopes for video conferences. MADCAP is a part of the Windows 2000 DHCP service configuration.

Microsoft Windows 2000 Certificate Services To support secure data conferences, you must install Windows Certificate Services on at least one computer within the Active Directory forest that contains T.120 multipoint control units that will host secure conferences. Certificate Services issues machine certificates to the MCUs and user certificates to users. The MCU uses these certificates to authenticate users for online conferences and to authenticate itself to other MCUs. After initially requesting certificates,

the MCU periodically receives certificates for new users or users whose certificates have changed.

Microsoft Internet Information Services (IIS) Microsoft Internet Information Services is required to host conference access Web pages.

Microsoft Windows 2000 Active Directory Service Active Directory is required to support conference resource objects and configuration objects.

Client Requirements

There are system and software client requirements for users who organize conferences and users who participate in conferences.

The recommended requirements are listed below. Clients meeting these requirements can take full advantage of Exchange Conferencing Server's features.

- Microsoft Windows 2000
- Outlook 2000
- NetMeeting 3.01
- IP –multicast-enabled network
- Internet Explorer 5.0 or other Internet browser. Browsers must be frames capable and have JavaScript enabled and be able to download ActiveX controls.

Conference participants will access different conferencing features, depending on which versions of these applications they use.

While these are the recommended requirements, there are minimum requirements that will still allow users to organize conferences and participate in data and video conferences.

Conference Organizers

The minimum software requirement for conference organizers is an e-mail application with a calendar, such as Outlook 97 (or later) and Outlook Web Access.

Data Conferencing Client

The following are the minimum software requirements for participating in a data conference:

- Frames-capable Internet browser with JavaScript enabled (such as Internet Explorer 4.01, or Netscape 4.5)
- T.120-compliant client application (such as NetMeeting)

Data Conferencing Provider supports NetMeeting 2.0, 2.1x, 3.0, and 3.0x. Additional data conferencing features are available with the later versions. For example, with versions prior to 3.01, Data Conferencing Provider automatically runs NetMeeting when the client accesses and connects to an online conference. NetMeeting is run as a top-level application. With NetMeeting 3.01, Data Conferencing Provider also hosts NetMeeting's data collaboration controls within the conference Web page if the Internet browser supports ActiveX controls. When you use NetMeeting 3.01 or above, you can participate in secure data conferences. NetMeeting automatically selects a public certificate installed on

the client computer. After authenticating the conference participant, NetMeeting encrypts the content of a data conference.

On computers without NetMeeting, Data Conferencing Provider prompts the user to start his or her T.120 client. Then Data Conferencing Provider sends an invitation from the data conference to the client.

Video Conferencing Client

The following are the minimum software requirements for participating in a video conference:

- Frames-capable Internet browser with JavaScript enabled (such as Internet Explorer 4.01, or Netscape 4.5)
- NetMeeting 2.1 or later (if you are not on a multicast-enabled network)

Clients accessing an online conference from a computer with Microsoft Windows 2000, on an IP-multicast enabled network, receive a multiparty, video image of the conference participants. These video images are embedded into the conference Web page using an ActiveX control.

Clients without Windows 2000 or a multicast-enabled network, must install NetMeeting 2.1 or later on their computers. Video Conference Provider connects these client computers into the video conference using a H.323 unicast NetMeeting call. Clients that connect in this manner receive the audio for five participants from the conference and a single video image of the conference participant who is speaking.

Multicast clients require a Windows 2000 operating system (OS). In addition, multicast video clients use a downloaded ActiveX control that runs in the Video Conference Provider frame of the Internet browser. Make sure your browser security settings allow ActiveX controls to be downloaded and run on client computers. Or, manually install ActiveX controls on the client computers.

Hardware Requirements

Review the hardware requirements for servers on which you plan to install Conference Management Service, Data Conferencing Provider, and Video Conferencing Provider. Also, review the hardware requirements for clients that will participate in data or video conferences.

Servers

The minimum requirements for servers on which you install Conference Management Service, Data Conferencing Provider, Video Conferencing Provider, or multipoint control units are:

- 133 MHz Pentium processor
- 128 MB of RAM

The recommended minimum requirements for servers on which you install Conference Management Service, Data Conferencing Provider, Video Conferencing Provider, or multipoint control units:

- 400 MHz Pentium processor

- 256 MB of RAM

A multipoint control unit installed on this hardware configuration with no other applications active can process approximately 500 simultaneous user connections.

Client Computers

There are minimum and recommended hardware requirements for clients that are participating in data and video conferences. The following sections outline these requirements.

Data Conferencing Client

The following are minimum hardware requirements for clients participating in a data conference:

- For Windows 95, a Pentium 90 processor with 16 megabytes (MB) of RAM
- For Windows NT, a Pentium 90 processor with 24 MB of RAM

The following are the recommended hardware requirements for clients participating in a data conference:

- For Windows 95, a Pentium 133 processor or better with at least 16 MB of RAM
- For Windows NT, a Pentium 133 processor or better with at least 32 MB of RAM

Video Conferencing Client

In order for multicast client computers to participate in video conferences, they must have the same hardware that is required for computers running Microsoft Windows 2000 Professional. Also, the following peripherals are required for video conferences:

- 56,000 bits per second (bps) or faster modem, ISDN, or LAN connection
- Sound card with microphone and speakers
- Video capture card or camera

The following are the minimum hardware requirements for multicast clients who are participating in video conferences:

- 133 MHz Pentium processor
- 64 MB of RAM

The following are the recommended minimum hardware requirements for multicast clients who are participating in video conferences:

- 266 MHz Pentium processor
- 128 MB of RAM

Video conference clients without Windows 2000, must use NetMeeting to participate in video conferences. Net Meeting uses H.323 to communicate with the MCU and bridge participants into the conference. The following are the minimum hardware requirements for H.323 clients:

- For Windows 95, a Pentium 90 processor with 16 MB of RAM

- For Windows NT, a Pentium 90 processor with 24 MB of RAM

The following are the recommended hardware requirements for clients using NetMeeting to participate in a video conference:

- For Windows 95, a Pentium 133 processor or better with at least 16 MB of RAM
- For Windows NT, a Pentium 133 processor or better with at least 32 MB of RAM

Video Conference Performance

Video conferences can have a large impact on CPU usage and memory usage for individual participants. The following tables show performance data for video conference participants on three different platforms. As you can see, the platform for video conference participants impacts the performance of the conference. You can use this data to establish what is an acceptable level of performance and evaluate the hardware of users who will be participating in conferences.

Pentium 166 with 64 MB of RAM

Number of Participants	CPU Usage (%)
1	56%
2	71%
3	79%
4	95%
5	100%
6	100%
7	100%

Pentium 300 with 128 MB of RAM

Number of Participants	**CPU Usage (%)**
1	19 %
2	23
3	30
4	36
5	41
6	47

Pentium 550 with 256 MB of RAM

Number of Participants	**CPU Usage (%)**
1	7 %
2	9
3	12

4	15
5	15
6	16
7	16

Also, there are other factors that can impact performance in a video conference, such as the amount of memory on your video card.

Permissions

To administer your Exchange Conferencing Server, you must have the following permissions.

Managing Exchange Conferencing Server

To manage and configure site-wide conference settings, Conference Management Service, Data Conferencing Provider, Video Conferencing Provider, and all multipoint control units, you must have read and write permissions on the conferencing site.

Exchange Conferencing Server Services

To start and stop services, such as Conference Management Service, multipoint control unit service, or H.323 service, you must have permissions to stop and start services on the servers on which these services are installed. You need to be a member of the Domain Admins group, or be logged on with the domain administrator account.

Resource Management

To install the Exchange Conferencing Server components, and to create and manage the conference calendar mailbox and any conference resources, you must have permissions to create domain user accounts.

DRAFT

DRAFT

CHAPTER 4

Component Planning

This chapter contains information on component planning for Conference Management Service, Data Conferencing Provider, and Video Conferencing Provider.

Conference Management Service

The number of conferencing sites needed for your organization and where to install them depends on your organization's network topology and demand for online conferencing.

Analyze the following aspects of your organization to decide how many conferencing sites you need and where to install them:

Anticipated schedule load Consider how Exchange Conferencing Server will be used within your organization based on existing network patterns. There may be obvious physical considerations in your organization, such as multiple data centers. For example, if you have e-mail servers at each of several data centers, consider installing Conference Management Service on these sites.

Logical separation of conferences Consider how your organization will use online conferences, and then create sites for different types of conferences. For example, you could create a conferencing site for conferences that are published to the Internet.

Multisite conference topologies Because only one Conference Management Service is active on a Windows 2000 site, consider balancing your user load across multiple sites by assigning users to sites according to their geographic location. Data Conference Provider uses the conferencing site architecture to assign a conference participant to the T.120 MCU that is closest to the participant's computer.

Initially, you can install one conferencing site, use the audit log files generated by Conference Management Service to monitor conference participation, and then decide if additional conferencing sites are required. If the audit log files indicate that you have too many conferences at one location, then install an additional conferencing site closer to the concentrated area to balance the load across your network. This enables Data Conferencing Provider to better create distributed conference topologies.

Single Conferencing Site

For an initial or pilot deployment, you can install all conferencing services on a single computer. As long as you create a virtual network address for the conference access pages, you can expand this pilot deployment to meet the needs of your organization.

The first Conference Management Service installed on a Windows 2000 site becomes the active host server for the conferencing site. You can install additional Conference Management Services on other servers, but only one is active on a site at any one time, as shown in Figure 4.1.

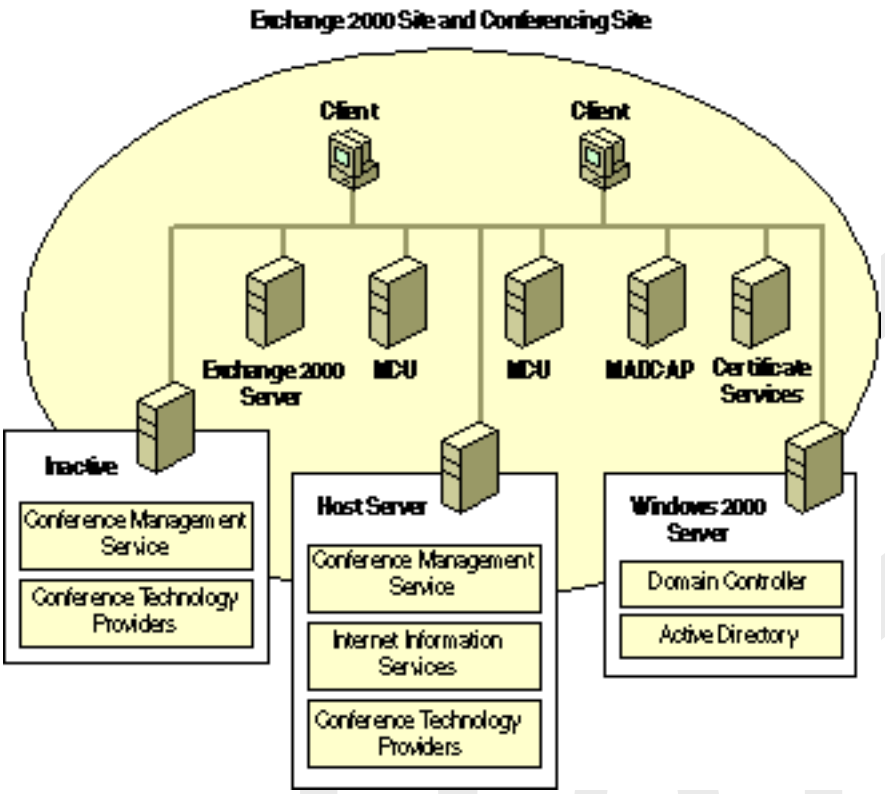

Figure 4.1 Single Conferencing Site

Figure 4.1 shows a conferencing site with the required components installed on the site: Exchange 2000 Server, Windows 2000 Server with Active Directory, MADCAP, and Certificate Services. You can install one or more conference technology providers on a conferencing site. Some providers, such as Data Conferencing Provider, include additional services, such as the T.120 multipoint control unit. These services can run on other servers. However, at least the base implementation of the conference technology provider code runs on the same server as the Conference Management Service.

Because all conference reservations and client requests are processed by a single Conference Management Service on a conferencing site, you must plan the server load to match the capacity of the server running Conference Management Service.

Before a conferencing site can host online conferences, you must:

- Create the site's conference calendar mailbox.
- Install any additional services required by the conference technology providers.
- Create the associated conferencing resources.

Multiple Conferencing Sites

If your organization has groups of people in more than one geographic location and more than one Windows 2000 site, you can create additional conferencing sites. Since each conferencing site has its own conference calendar mailbox, you must create conferencing resources and configure network addresses for the conference access pages for these

additional sites. Creating additional conferencing sites helps to balance network load and improve performance.

The distributed nature of the components within a conferencing site offers great flexibility in the deployment of Exchange Conferencing Server. By associating conferencing resources with a specific Conference Management Service, the associated conference technology provider resources and public conference lists can be separately managed. For example, creating a separate conferencing site within your organization with connectivity to the Internet allows the conference schedule to be accessible from the Internet. This allows users who might participate in conferences through the Internet to see the list of public conferences. They do not, however, see conferences internal to your organization.

Exchange Conferencing Server must be installed on a Windows 2000 site. However, if you plan to create more than one conferencing site or install Data Conferencing Provider with connectivity to the Internet, you must:

- Create an Active Directory Connector Connection Agreement for account replication
- Configure the site subnet definitions using Active Directory Sites and Services.

If there are no other Windows 2000 sites, then all users and all conferencing servers belong to the local site. In this case, Exchange Conferencing Server cannot optimize the conferencing site by identifying the closest server. If your organization requires only a single site, and for security reasons you don’t want to expose your primary Exchange server to the Internet, define a second site to identify user connections originating from the Internet.

Exchange Conferencing Server with Earlier Exchange Systems If you expect users on Exchange 5.5 Server to schedule online conferences, you need an Active Directory Connector Connection Agreement to replicate conferencing resources for Active Directory to the Exchange 5.5 directory. For more information on creating an Active Directory Connector Connection Agreement, see Exchange 2000 online help.

Conference Technology Provider Location

Along with the Conference Management Service, a conferencing site has one or more conference technology providers. The ECS installs both Data Conferencing Provider and Video Conferencing Provider when you install Conference Management Service. You can select which conference technology provider you create resources for and which providers are active within a specific conferencing site. You can install third-party providers after you install Conference Management Service, but only on the conference site in which you will be using those types of resources. For example, if you create a separate conferencing site for online conferences with Internet participants, create only Data Conferencing Provider resources, because video conferencing is not widely used over the Internet.

Conference Access Pages

Each conferencing site has a set of conference access pages. Participants use conference access pages to participate in conferences scheduled on each site. The actual conferences may span multiple conferencing sites.

Conference access pages are installed on an IIS server. The conference invitation includes the conference URL that participants use to access the conference. The conference URL is

composed of two parts: the base address and the conference identifier. The conference identifier is appended to the base address.

URL Element	Example
Base Address	http://<*server_name*>/conferencing
Conference Identifier	/default.asp?<*conference_parameters*>
Conference URL	http://<*server*>/conferencing/default.asp?<*conference_parameters*>

Where <*server_name*> is the name of the IIS server that hosts the conference access pages and <*conference_parameters*> is a group of parameters that define the conference.

The base address is listed on **Conferencing Site Properties.** Click the **Conference Settings** tab and the base address is listed under the **Access URL for user connections.** This URL is the base address of the IIS server that hosts the conference access pages and, by default, is based on the NetBIOS name of the IIS server.

The conference identifier includes several parameters that define the conference, such as a unique conference id, and in some cases also conference start time, and the password.

A single Internet Information Services (IIS) server is sufficient, in most cases, for hosting all the users within a conferencing site. However, either for reasons of redundancy or deployment within very large organizations, it may be necessary to place the conference access pages on more than one server. Each server should be addressed using the same virtual network name as the one configured on Conference Management Service.

If your IIS server is expected to accept connections from Internet participants, you must configure the virtual root for private conferences to allow Internet participants to participate in private conferences using basic authentication.

To configure the private conference virtual root:

6. On the Start menu, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
7. In the console tree, double-click ***ServerName***, and then click **Default Web Site**.
8. In the details pane, right-click **ConferencingPrivate**, and then click **Properties**.
9. Click the **Directory Security** tab.
10. Under **Anonymous access and authentication control**, click **Edit**.
11. On **Authentication Methods**, clear **Integrated Windows Authentication**.

This allows Internet users to participate in private conferences using basic authentication.

Warning Remember that basic authentication sends user's credentials, including the password, in plain text format.

Default Conference Access Pages

Use a logical server name for the computer hosting the conference access pages, even if the conference access pages are hosted on the server with an active Conference Management Service. This computer name is embedded in all scheduled conferences. If

you accept the default Windows Internet Naming Service (WINS) network address, then this address must always be used. The network address of these pages is included in the conference access URL that is sent to conference invitees. It is important that this network address does not change; otherwise, all conference definitions become invalidated. To prevent this, define a virtual network name, using DNS, for the computer hosting the conference access pages. You must modify the address defined by Conference Management Service in order to use this virtual network name.

If you plan to host the conference access pages on the same server on which you install Conference Management Service, you do not need to change the default conference access URL. If you change the conference access URL to refer to a different server, you must first install Conference Management Service on that server, then redirect client requests for previously scheduled conferences to the URL on the new IIS host server or change the DNS server settings to point to the new IIS server.

Scalability

A single conferencing site with conference access pages installed on the default host server is adequate for most companies. However, very large companies that place a heavy demand on their Exchange Conferencing Server can designate a single computer or group of computers to process conference access requests.

Depending on your network bandwidth, server performance, and number of online conferences, a single server with Conference Management Service can maintain from thousands to hundreds of thousands of users on a site. However, if the network is segmented and geographically dispersed, with low bandwidth links between the remote locations, define a separate Windows 2000 site on each network segment and install ECS on each site where conferencing services are used regularly. This configuration can scale to support all conferencing needs.

Conference Calendar Mailbox

The conference calendar mailbox contains the definitions of all conference schedules within a conferencing site. This is critical information and must be available to Conference Management Service at all times. To prevent data loss, place the conference calendar mailbox in it's own Exchange storage group. This minimizes downtime because you only have to restore one storage group in the event of any disk failures.

If you apply storage limitation policies to the Exchange mailboxes, verify that the conference calendar mailbox has enough storage to hold the required number of online conference definitions.

Because all scheduled conferences within a conferencing site are stored in the conference calendar mailbox, you must regularly purge or archive historic conference definitions. You can create an Outlook profile for the conference calendar mailbox and archive older schedule information to keep storage space available.

Conference Resources

Each Conference Management Service manages a set of conference resources. Conference resources represent the physical resources that the conference technology provider provides during an online conference. Online conferences consume varying physical resources depending on the type of online conference. Conference technology

providers refer to conference resources by the type of physical resource that an online conference consumes. For example, for data conferences, a user connection to a multipoint control unit is the consumable resource. For video conferences, a stream of audio and video is the consumable resource.

After you create a conference resource, assign the resource to conference technology providers in your conferencing site. Conference technology providers have properties associated with the resource, such as number of user connections allowed, or video resolution, that define characteristics of conferences that use the resource.

Create only one conference resource for a specific configuration. For example, you only need one conference resource to represent a data conference for 10 people. Unlike the address book entry that is created for a physical meeting room, conference organizers can reserve a conference resource many times before it becomes busy. Resources are properties of a Conference Management Service within a specific conferencing site. Only the conference technology providers installed on the conferencing site can be assigned to a conference resource.

Because public conferences within your conferencing site are listed on conference access pages, you should control who can create conferences that will be accessed by people outside your organization. For those 'Internet' resources, the name should be in some way distinguished to inform the conference organizer. See Naming Conventions later in this chapter.

When is a resource busy

To schedule resources, Exchange Conferencing Server uses a resource model and rules of availability that include free and busy information and resource costs. Each conferencing resource publishes free and busy information to the Exchange Free/Busy public folder. Each conferencing technology provider uses the free and busy information and the resource cost to determine if it can reserve a specific resource. After a conference technology provider reserves a resource, it calculates resource availability for the remaining resources. If a conference organizer requests conference resources for another conference and the conference technology provider cannot accept the cost of this additional conference, the resource is at capacity and shows as busy.

For example, you have two conference technology providers. Provider A has 50 resource units available and provider B has 100 units. You have the following resources:

- A (10),
- B (10),
- A (40),
- A+B (20)

The resource costs are in parentheses.

Initially all resources publish a free status. Someone schedules a conference using resource A+B (20). The cost of the resource is reduced from each provider's total. Provider A now has 30 units available (50-20=30) and provider B has 80 (100-20=80). Since provider A has 30 units available, there are not enough resources for someone to schedule a conference using the A (40) resource. Provider A communicates that the A (40) resource is busy, but the A (10) resource is available.

Naming Conventions

You must define a naming convention that describes the features of each conference resource. Before creating your naming convention, consider the following:

- Are there multiple Conference Management Services within your organization that publish resources for their conferencing site?
- What conferencing features are available from the conferencing resources?
- Do any of the resources limit the number of participants?
- Are there restrictions on who can reserve conference resources?

You can name resources based on their location or the technology that they provide. It is helpful to include the number of participants that the resource can host in the name of the conference resource, so when organizers are looking for a resource in the Address Book, they can easily find a resource with the capacity to host their conference.

Location You can configure a conference resource to allow participants within a restricted geographic region to participate in a conference. You can name a resource using the geographic name, conferencing feature, and number of participants. For example:

- Redmond virtual team conference (10)
- Redmond video conference (8)
- New York teleconference (12)

Technology You can name a conference resource based on the technology or conferencing feature that it provides. This is a useful naming convention for conference organizers. For example:

- Online data/video (10)
- Online video [CIF] (4)
- Online telephone/data (12)
- External data (10)

In each case, the size indicates the maximum number of participants.

Reliability Planning

You must create a reliability plan to help maintain a healthy and available Exchange Conferencing Server. Use this plan to define the level of redundancy and what action to take if a component fails. You must understand the possible points of failure in an Exchange Conferencing Server and your options for fail-over strategy.

The following table summarizes the key components in Exchange Conferencing Server, failure types you could encounter, and what you can do to prevent or recover from a failure.

Component	Failure	Recovery or Fail-Over Options
Conference Calendar Mailbox	Disk	Place data on a redundant RAID array.

		Place mailbox in separate storage group and backup frequently.
Conference Calendar Mailbox	Exchange	Put the Exchange server into an active/active cluster.
Conference Management Service	Server/Service	Install an additional Conference Management Service on a backup server, so that you can switch to the backup server if necessary.
Conference Access Pages	Server/Service	Use Windows load-balancing for the IIS service. Install conference access pages on a backup server and change configured DNS address of the conference location to the backup server.
T.120 Multipoint Control Unit	Server/ Service/ Network	Ensure that each conferencing site has multiple servers that can accept client connections for the same user locations. ECS provides automatic fail-over for MCUs.
MADCAP Service	Server/ Service/ Network	Install more than one MADCAP server and specify scopes on the conferencing resources for both servers.

Backup and Restore

Exchange Conferencing Server places configuration data in Exchange and Active Directory.

Exchange Exchange Conferencing Server places mailboxes for the conference calendar and conference resources in the Exchange mailbox store.

Windows Active Directory Active Directory contains objects for the conference resources and conference calendar mailboxes.

To recover from catastrophic failure, you must follow the backup and restore strategies for each of these components. For information on backup and restore strategies for these components, see Exchange 2000 Server and Windows 2000 online documentation.

Best Practices

To plan your Exchange Conferencing Server deployment, consider the following strategies and practices:

Network Topology If you plan to hold conferences with anyone outside your organization (for example, on the Internet), consider placing IIS on an independent computer whose DNS host name can be resolved by both internal and external clients.

Conference Calendar Mailbox Keep the conference calendar mailboxes on the server with the active Conference Management Service. Performance may dramatically decrease if the calendar mailboxes are on different servers.

Conference Resources and Conference Calendar Mailbox On the server running Conference Management Service, make conference resources and the conference calendar mailbox the only mailboxes. If you must share this server with user accounts, put the conference resources and the conference calendar mailbox in a separate message database. This will minimize downtime if you need to restore scheduled conferences or move them to another message database.

Naming Conventions Use descriptive names that distinguish your conference resources from physical meeting rooms. For example, you can use Virtual TeamConference (10) for the display name of a data and video conference resource with a maximum participation size of 10. You can define multiple resources of the same type but in different sizes, in order to use resources more efficiently. If you have multiple conferencing sites, use resource names to describe their locations.

Sites with Multiple Subnets If your site has multiple subnets and some of the links are slow, place one or more multipoint control units on each subnet. Configure the multipoint control units to accept connections only from the users of that subnet.

IIS Location Even if you are going to run the IIS server on the same server as Conference Management Service, change the meeting access location address to a virtual name for that computer. This prevents conference participants from losing access to scheduled conferences if you decide to move IIS. You need to change the mapping on the DNS server only to point the virtual name to the new IIS server.

Initial Implementation Consider a phased rollout of Exchange Conferencing Server if you are new to online conferencing. Deploy the service on one server and give access to a single group. Then, add additional servers and groups as demand increases for the service.

Data Conferencing Provider Planning

How you deploy Data Conferencing Provider depends on the topology and other characteristics of your network. Also, you must decide how to prioritize the different properties of Exchange Conferencing Server. For example, do you want to confine conference network traffic to a specific area of your network? Do you consider the cost of conference traffic across the network infrastructure higher than the cost of managing additional decentralized servers?

The optimal number and placement of multipoint control units depends on your network topology and how multipoint control units are used. You should consider the number of conference participants and their location on the network, the cost of placing additional conference traffic on the network, the level of redundancy for fault tolerance, and service performance requirements.

The following criteria affect the deployment architecture for data conferencing:

- Windows 2000 site architecture
- Working with remote data conferencing sites
- Network considerations

Windows 2000 Site Architecture

Exchange 2000 Conferencing Server uses the Windows site as the outermost layer of the conferencing site. When you use Exchange Conference Manager, you manage a conferencing site. The Windows site defines the location of servers and conference

participants on the network and the connectivity between them. Data Conferencing Provider uses this information to decide which multipoint control unit to assign to conference participants.

The Windows site architecture is constructed using Windows Sites and Services. If your Windows organization is using any form of directory replication, this architecture is defined. Typically, a site defines the subnet addresses of the computers on your networks that are interconnected by high bandwidth and persistent connections. If you do not have Windows 2000 sites defined, then you must verify that all conferencing servers are connected by high bandwidth and persistent connections.

The first server that has Conference Management Service installed in the site is considered the top-level server on Exchange Conferencing Server. The Windows site on which this server is installed is the root node for data conferencing servers. The Data Conferencing Provider code always resides on the same computer as Conference Management Service.

Exchange Conferencing Server defines the servers that host the multipoint control units according to the conferencing site and the Windows site in which it resides. When an MCU is installed on a server, it tries to assign itself to a conferencing site within the Windows site.

Working with Remote Data Conferencing Sites

You can have multiple conferencing sites within your organization. Data Conferencing Provider uses this architecture to decide on the preferred network locality of a user who asks to join a conference. When a conference participant asks to join an online conference scheduled at one location, Data Conferencing Provider searches for a conferencing site on the participant’s Windows site. If there is a multipoint control unit on the conference participant's Windows site, the participant is referred to that conferencing site.

Network Considerations

The cost of network bandwidth between Windows sites and subnets within a conferencing site impacts where you install MCUs. When you have conferences that span Windows sites and subnets, Data Conferencing Provider helps to reduce the cost of your network connection by directing the unicast client connections to a single MCU. Then Data Conferencing Provider creates a unicast connection between the MCU and an MCU in the other Windows site or subnet. By creating a single source of conference data, ECS provides a network model that is more scalable and uses network bandwidth more efficiently.

Conference Participants Location

When connecting a conference participant to the closest MCU, the data conferencing provider considers the following:

- Is the participant joining a conference from a remote location that has a conferencing site?
- Is the participant joining a conference from a location that is local to the conferencing site?
- Has the administrator defined visibility restrictions on the MCU to which a participant can connect?

When a participant from one conferencing site attempts to join a conference on another conferencing site, the hosting conferencing site directs the user to his or her local site and initiates a connection between the two sites. This creates a single instance of the

conference data between the two sites. This is very useful if you have clients trying to participate in a conference across a slow network link, as shown in figure 4.2.

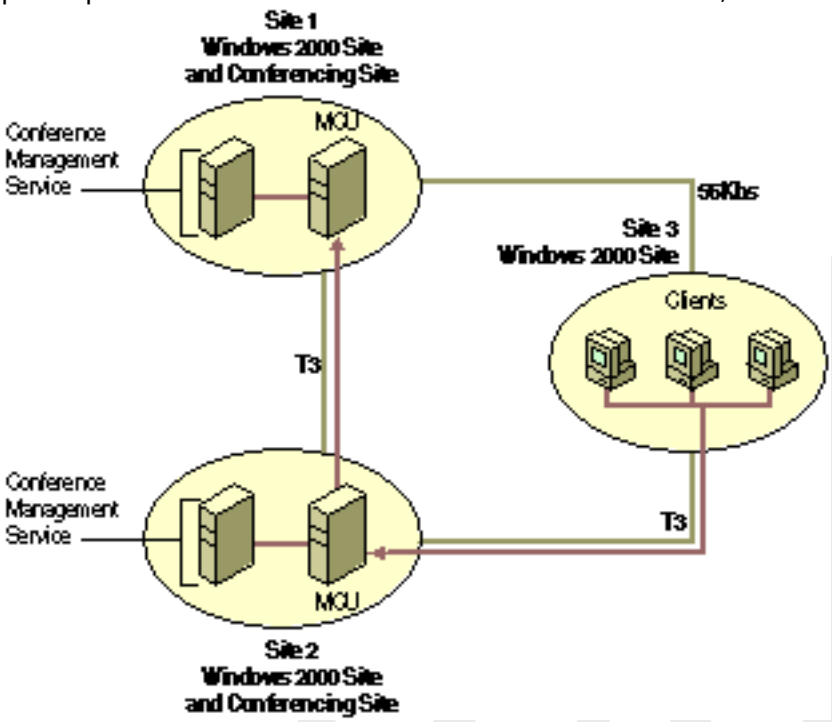

Figure 4.2 Multipoint Control Unit Affinity

In figure 4.1, the clients on site 3 are invited to a conference on site 1. There is a slow connection between site 3 and site 1 but fast connections between site 3 and site 2, and site 2 and site 1. To improve the performance of the conference, use MCU affinity to connect the clients on site 3 to the MCU on site 2 and then to the conference on site 1.

If a participant attempts to join a conference from a Windows 2000 site that does not have a conferencing site, and if the Windows site has been given affinity to an MCU on another site, the participant is considered to be local to that site. Otherwise, the participant is remote to the hosting site and connects to an MCU on the conferencing site that is configured to accept remote connections.

Through administrative settings, you can restrict access to an MCU based on a set of subnet mask pairs. Only users whose IP addresses match a defined subnet can connect to the MCU. In this way, administrators can divide a Windows 2000 site and direct participants to a specific MCU.

Conferencing Across a Firewall

You can configure Data Conferencing Provider to support conferences hosting Internet or remote site participants who are connecting over a corporate or site firewall.

Each MCU can be configured with a different network name, which is used by participants to connect to the MCU from each of the three regions separated by these firewalls.

All users on the local conferencing site use the local network name, while users remote to the conferencing site use the remote network name. Users from the Internet use the Internet network name. Establishing separate network names provides two methods for bridging the security regions. The simplest is to connect each network card to the separate network region. Then, configure each network name to be the IP address, or associated DNS name, of each of these network cards. Clients that attempt to join

conferences from each region are given the network address of the network card for which they have access.

Alternatively, some firewall products can be configured to implement a reverse packet filter for the T.120 connections on port 1503 and target connection requests to the MCU. In this case, the MCU is connected to the Intranet and the external clients refer to the MCU with the network name of the firewall.

Secure Conferencing

To participate in secure conferences, participants must use NetMeeting 3.01 or later and Microsoft Internet Explorer 4.01 or later. To support secure conferences, you must install Windows 2000 Certificate Services on at least one server in the domain. Certificate Services provides a certificate authority that grants certificates to users to authenticate them for secure conferences.

Reliability Planning

To improve the reliability of data conferencing in your organization, install multiple MCUs to accept connections from the same groups of users. There is no need to place MCUs in a cluster however, because Data Conferencing Provider provides automatic fail over for the MCUs on the site.

Because MCUs exchange Distributed Component Object Model (DCOM) calls with Data Conferencing Provider, make sure that the MCUs on your Windows 2000 site have fast connections to the server that has the active Conference Management Service.

You can use the ECS audit and application logs, and System Monitor counters as information sources for assessing the current reliability of your Data Conferencing Provider infrastructure. In particular, the MCU application logs provide statistics on the number of software, hardware, and network failures, and MCU downtimes. The System Monitor counters indicate the connection speeds and the volume of DCOM traffic.

Scalability and Performance

The audit log files and System Monitor counters provide valuable information on the MCU load dynamics, average connection delays, and other performance characteristics of Data Conferencing Provider. You can use this information to plan how many and what type of MCU servers to include in your organization.

Data Conferencing Provider allows you to increase the number of MCUs on the site. However, you must make a trade-off between the number of MCUs and individual server performance. If you deploy many MCUs, accepting connections from the same groups of users using relatively low performance servers, Data Conferencing Provider automatically balances the load by choosing the MCU with the lightest load to host the conference. Then, it connects all of the local participants of that conference to the same MCU to minimize conference traffic. This continues until a configurable maximum load level for the MCU is reached. The next connection request is directed to another MCU with the lightest current load.

Because of the threshold limit, deploying an MCU on a computer with a faster processing speed produces conferences that span fewer MCUs, therefore causing shorter delays for conference payload traffic. When you deploy a larger number of MCUs on computers with slower processing speeds on a site, you get better reliability and fault tolerance.

Multipoint Control Unit

When a participant accesses a conference, Data Conferencing Provider directs him or her to a specific MCU, depending on the network address of the participant's computer. Data Conferencing Provider gets the client's network address from the Web browser. Because of this, client computers within a conferencing site should be configured to bypass any proxy server when accessing the conference access page server. Users from remote conferencing sites can use an inter-site proxy server if the following conditions are true:

- Their proxy server is within the remote Windows 2000 Site.
- Within his or her site, the participant has local access to the server with the conference access pages.

Using the participant's IP address, Data Conferencing Provider looks for conferencing sites within the organization. If it finds a conferencing site that has preferred ownership of the participant's location, then it connects the participant to the local conferencing site, supplying the conference name and network name of the local MCU on which the conferencing sites can be linked. On the remote conferencing site, Data Conferencing Provider selects the best MCU for the conference.

If the user is accessing the data conference from a Windows client running Internet Explorer and NetMeeting, he or she automatically connects to the MCU hosting the conference. If the user does not have these applications, the MCU sends a T.120 message to the client's IP address, inviting them to the conference. If this invitation fails, the details for the conference appear on the Web page, allowing the user to manually call the T.120 conference.

Multipoint Control Unit Security

You can configure each MCU to restrict user access to its conferences in several ways. By default, an MCU does not allow connections from the Internet, but does allow local and remote connections. An MCU can distinguish between user connections from a local site, a remote site, and the Internet. You can configure an MCU to restrict or allow access from any of these categories. Also, a set of network addresses can be configured for any combination of these categories. The MCU can deny connections from clients that don't belong to the defined set of network addresses. Data Conferencing Provider directs these clients to the next best MCU in the organization.

You can also specify an MCU for clients to connect to if the clients are in a Windows 2000 site that is not a conferencing site. For procedures, see *Configuring MCU Connections and Types*, later in this chapter. Configure this using

With so many options for managing access to MCUs, it is important to evaluate your requirements, network infrastructure, and conferencing patterns to decide which options are best for your organization. For example, consider the following:

- Is network load more important than fault tolerance for Data Conferencing Provider?
- Is easier management of the overall network more important than optimal use of network resources?

Network Deployment

This section contains examples of backboned, hub and spoke, and multiple site deployments of MCUs. Refer to these to help you decide how to use MCUs in your organization.

Backbone Topology

Consider a backbone deployment in which all clients have a low-cost, high-bandwidth connection to a centralized network. Usually, this kind of deployment has network services, such as e-mail and database services, in a centralized data center. In this case, the components of ECS would also be placed in the centralized location. Install MCUs to provide load-balancing and redundancy for all network clients.

Consider a backbone deployment if you plan to use Data Conferencing Provider on only one Windows 2000 site, and you are not concerned about inter-subnet network traffic. The backbone topology places Conference Management Service and all the MCUs on the backbone network. This improves resource management, load balancing, fault tolerance, and administrators have better control servers in case there is a change made to the network infrastructure. However, there is more network traffic between subnets.

> **Note** In the following figures, IIS is shown on the same server as Conference Management Service. This is not a requirement. You just need IIS running on the same site as Conference Management Service.

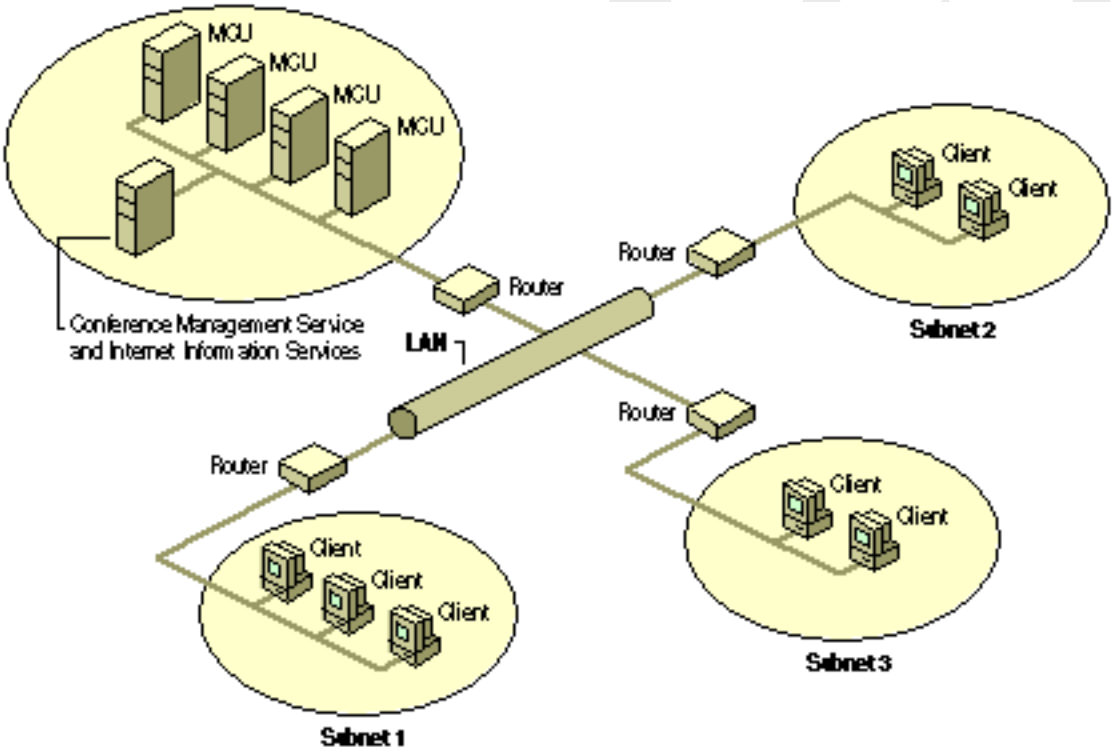

Figure 4.4 Backbone Topology

Hub and Spoke Topology

If you are concerned about traffic between subnets, consider a hub and spoke topology. Place Conference Management Service in the hub, and then place one or more MCUs on the subnets with conferencing users. This layout routes conference traffic over a single link. This topology improves network load but compromises load balancing and fault tolerance. A hub and spoke topology can be more efficient than a backbone topology if most of conference participants are on the same subnet. In this case, most of the network traffic happens within the subnet.

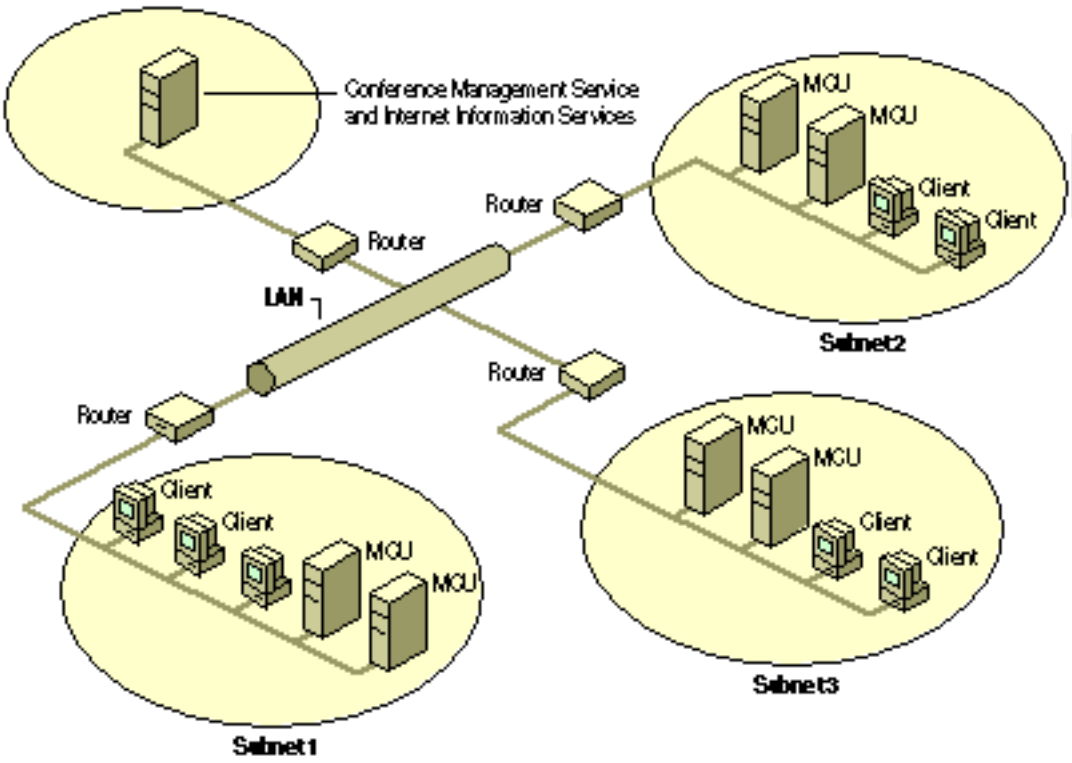

Figure 4.5 Hub and Spoke Topology

Decentralized Topology

If you have multiple sites that could have conferences occurring at the same time, consider a decentralized deployment. In each site, there is a Conference Management Service and one or more MCUs. If there are firewalls between the sites, a proxy MCU must be defined on each site.

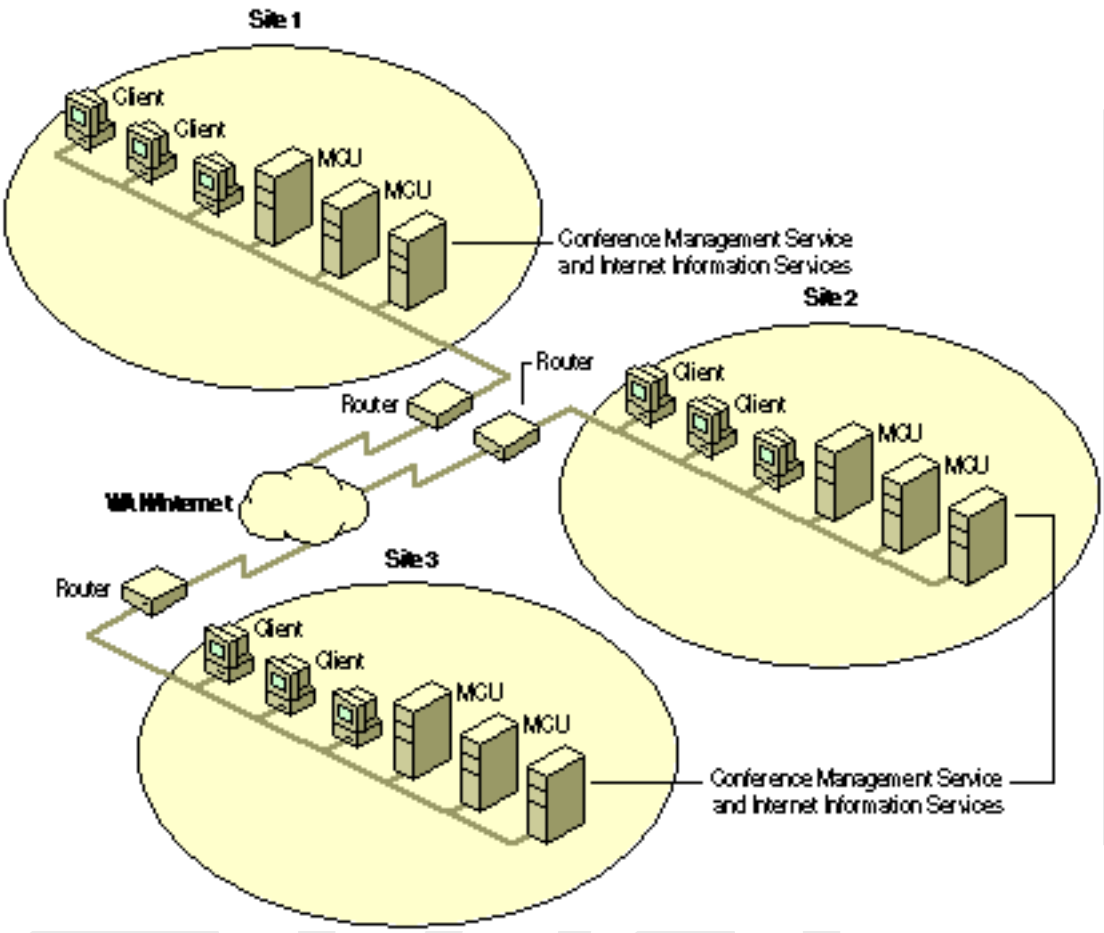

Figure 4.6 Decentralized Topology

If you want to further limit inter-site bandwidth usage, dedicate an MCU on each site for remote connections. This ensures that a single instances of data travels across a WAN link.

When planning a decentralized deployment, consider that conference organizers can only reserve conference resources within their sites. If users participate in data conferences on remote sites, they are connected to local MCUs but the impact that their connection has on MCU capacity is not reflected in resource availability on the local site. Even though they are participating in a remote conference, since their connection is through a local MCU, they still have an impact of the capacity of the local MCU. Thus, if you expect a large number of inter-site conferences, be conservative when setting the **Maximum number of scheduled connections** for an MCU. You can configure this setting on **Data Conferencing Provider Properties** on the **General** tab.

MCU Connections and Types

There are many ways you can customize MCUs to meet the needs of your organization. You can assign specific MCUs to different tasks on your conferencing site. The following procedures illustrate some common uses for MCUs.

In the following procedures, you must navigate to the MCU you want to configure.

To navigate to an MCU:

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **Conferencing Server Administration** ***PLACEHOLDER****.
2. In the console tree, click **Exchange Conferencing Services**, click ***Site_Name*** **Conferencing Site**, and then double-click **Data Conferencing Provider**.
3. In the details pane, right-click the T.120 MCU server you want to configure, and then click **Properties**.

Local MCU A local MCU accepts only connections from participants whose computers are on the same Windows 2000 site.

To configure a local MCU:

1. Navigate to the MCU you want to configure (as previously explained).
2. On the **General** tab of **MCU Properties**, verify that **Accept client and T.120 MCU server connections from remote sites** and **Accept client connections from the Internet** are cleared, and that **Accept client connections from local sites** is selected.

Local MCU with subnet scope restrictions This is an MCU that only accepts connections from participants on specific subnets on the site. You control access by defining subnets.

To configure a Local MCU with subnet scope restrictions:

1. Navigate to the MCU you want to configure (as previously explained).
2. On **MCU Properties**, on the **General** tab, verify that **Accept client connections from local sites** is selected, and then click **Restrict Visibility**.
3. Click the **Visibility** tab, click **Add**, and then type the network address and subnet masks for your scope restrictions.

MCU with site affinities An MCU with site affinities treats connections from specific Windows 2000 sites as though they were on the same site. Use an MCU with site affinities to designate an MCU with a faster connection to a particular site as the preferred MCU for participants on that site.

To configure an MCU with site affinities:

1. Navigate to the MCU you want to configure (as previously explained).
2. On **MCU Properties**, on the **General** tab, under **Accept client connections from local sites**, click **Sites**.
3. On **Local Sites**, under **Available**, select the site you want, and then click **Add**.

Inter-site connector MCU An inter-site connector MCU serves as a bridgehead between remote Windows 2000 sites. This MCU accepts connections from remote MCUs and remote participants if ECS is not available on their sites.

To configure an inter-site connector MCU:

4. Navigate to the MCU you want to configure (as previously explained).
5. On **MCU Properties**, on the **General** tab, clear **Accept client connections from local sites**. By default, the option is selected.
6. Verify that **Accept client connections from the Internet** is cleared. By default, this option is cleared.

Internet connector MCU An Internet connector MCU accepts connections from Internet users.

To configure an Internet connector MCU:

7. Navigate to the MCU you want to configure (as previously explained).
8. On **MCU Properties**, on the **General** tab, click **Accept client connections from the Internet**, and then verify that **Accept client connections from local sites** and **Accept client and T.120 MCU server connections from remote sites** are cleared.

   Important note: If you configure an MCU to be visible from the Internet, and you have only one Windows 2000 site defined in your organization, you must create a second Windows 2000 site and deploy the Internet visible MCU on that site. Otherwise, Internet users are considered local by Data Conferencing Provider.

Video Conferencing Provider

If you plan to use video conferences in your organization, you will have to ensure that your users are on multicast-enabled networks, or that they can be bridged into a video conference.

The following topics will help you implement video conferencing in your organization:

- Multicast basics
- DHCP and MADCAP configuration
- Network Configuration
- Resources
- Best Practices

Multicast Basics

Multicast clients have the most feature-rich user experience with video conferencing and ECS. The following sections provide background information on IP multicast, multicast addresses, time-to-live value, multicast groups, multicast scopes and IP addresses that are reserved for multicast.

IP Multicast

IP multicast is an extension to the IP network layer protocol defined in RFC 1112. It provides an efficient way of transmitting packets on the network from one or more sources to many destinations.

There are three basic modes of transmitting packets over an IP network: unicast, broadcast, and multicast.

In unicast mode, packets are transmitted over a point-to-point connection. If there is more than one recipient for the packet, several point-to-point connections are established and a copy of each packet is sent to each recipient.

In broadcast mode, a single copy of a packet is sent to the entire network, including subnets that don’t have recipients for the packet. Thus, extra traffic is created that consumes valuable network bandwidth.

In multicast mode, a single copy of the data is transmitted to subnets that have a recipient host subscribed to the session. Hosts subscribe to the session by joining a multicast group, which they do by propagating (through Internet Group Membership Protocol) a pair of addresses—multicast address and recipient's IP address—to the routers on the network.

Multicast Address

Class D IP addresses, in the range 224.0.0.0 to 239.255.255.255 are called multicast addresses. Packets sent to an address in this range are not addressed to a specific host. Any host that has knowledge of a specific multicast address can join a multicast group identified by this address. Once a host joins, routers start forwarding all packets that it encounters to the subnet on which the host resides. The host can then pick up the packets being sent to that address. A host can become a member of any number of multicast groups.

Time-to-Live Value

It is not a good idea to distribute all packets sent to all multicast addresses throughout the world. Multicast packets have a specific lifetime. The Time-to-Live (TTL) value identifies the lifetime of these packets. Every time a router is hit in the path of the packets, the TTL value is reduced by one, and if the value is zero, the router does not forward the packets any further. This means that packets with a TTL value of 1 are distributed within the subnet only. Multicast datagrams with a TTL value greater than one can be delivered to more than one subnet if there are one or more multicast routers attached to the first subnet.

Multicast Group

An IP multicast group, also known as a host group, is a set of hosts that finds IP traffic destined for a specific multicast IP address. Multicast IP traffic is sent to a single Media Access Control (MAC) address but processed by multiple IP hosts. A given host receives all packets sent to a specific IP multicast address.

Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast groups. The membership of a host group is dynamic. Hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group. A host may be a member of more than one group at a time.

A host group may be permanent or transient. A permanent group has a well-known, reserved IP address. These addresses are registered with the Internet Assigned Numbers Authority (IANA). (For more information, see *Reserved Addresses*, later in this chapter.) It is the address, not the membership of the group that is permanent; at any time, a permanent group may have any number of members, or no members. The IP multicast addresses that are not reserved for permanent groups are available for dynamic assignment to transient groups that exist only as long as they have members. Members of a host group can span IP routers across multiple networks. This requires IP multicast support on the IP routers and the ability for hosts to register their group membership with local routers. Host registration is accomplished using IGMP.

For a host to receive IP multicasts, a client application must inform the local router that the application will be receiving multicasts at a specified IP multicast address. If the network technology supports hardware-based multicasting, then the client application signals the network interface card to pass up packets for a specific multicast address. With Ethernet, the network interface card, is programmed to respond to a multicast MAC address corresponding to the desired IP multicast address.

In order to facilitate IP multicast between subnets, the routers must be multicast aware. Routers maintain special routing tables enabling them to decide whether to forward

multicast traffic to the specific network or not. Routers propagate routing information and create a router topology, known as a spanning tree, for each multicast session. The spanning tree is constructed so that a single path exists between any pair of participating routers, without any loops.

Multicast Scope

A range of multicast addresses and an associated TTL define a multicast scope. The scopes used for video conferences are retrieved from the scopes defined on the organization's MADCAP servers. Using scopes, in conjunction with configuration of routers, you can limit the reach of multicast packets on the network. You can apply additional restrictions by configuring boundary routers for specific multicast scopes.

Reserved Addresses

The following table is a partial list of Class D addresses reserved for IP multicasting and registered with the Internet Assigned Numbers Authority (IANA). These are the addresses of the permanent, well-known groups mentioned above.

Multicast Group	IP Multicast Address	Description
Base address	224.0.0.0	Reserved
All hosts	224.0.0.1	Contains all systems on the same network
All routers	224.0.0.2	Contains all routers on the same network
Network Time Protocol	224.0.1.1	Distributes time-clock data used to synchronize time on a group of computers
RIP version 2	224.0.0.9	Distributes routing data between a group of routers that use the version 2 raster image processor (RIP)
WINS server	224.0.1.24	Supports auto-discovery and dynamic configuring of replication for WINS servers

A multicast router does not forward multicast datagrams with destination addresses from 224.0.0.0 through 224.0.0.255 regardless of their TTL value. This address range is reserved for routing protocols and other low-level, topology discovery or maintenance protocols. These include gateway discovery and group membership reporting protocols.

DHCP and MADCAP Configuration

Although MADCAP is packaged with the DHCP service, DHCP and MADCAP are independent of each other. You can use a MADCAP server to provide multicast addresses and run DHCP on other servers on your network.

For networks using domains, you must authorize the DHCP service in the domain's directory service database. This prevents users from setting up unauthorized DHCP services. This is not necessary if the server has been authorized already (for example, if it is already functioning as a DHCP server).

To have the DHCP server allocate multicast addresses using the MADCAP protocol, create a new multicast scope. After creating a new multicast scope, associate it with a TTL. For more information on configuring DHCP and MADCAP, see your Windows 2000 documentation.

Multiple MADCAP Servers

To support and configure Video Conferencing Provider, you must have MADCAP installed on one or more servers. Configuring multiple MADCAP servers can improve server reliability and network efficiency; if one MADCAP server is down, another one can deliver the MADCAP service to your conferencing site.

If you have MADCAP installed on more than one server on your network, verify that the multicast IP scopes configured on the servers do not overlap. Also, since each of the IP scopes is also associated with a lease expiration period and advertising scope settings, configure each type of multicast IP scope you want to have on two or more MADCAP servers.

Network Configuration

To use Video Conferencing Provider, your network needs to be multicast-enabled, and you need to configure multicast addresses. If this is the first IP multicast deployment in your enterprise, you may need to reconfigure some of your routers. However, if you have previously deployed multicast applications such as NetShow, your network may already be prepared for using multicast addresses.

If your network routers support Resource Reservation Setup Protocol (RSVP), you can configure the quality of service (QoS) policy to allocate network bandwidth. You can apply the policy to the network, each subnet or individual users. Use Windows 2000 QoS Admission Control to manage the policy. For further information on how to configure QoS policy, see your Windows 2000 online documentation.

When deciding on the maximum number of simultaneous connections allowed and configuring the QoS policy, consider the bandwidth of your network and how you will use Video Conferencing Provider in your organization. Are there going to be conferences that require all participants to send video and audio? What percentage of conferences will be audio-only?

Try to calculate the peak video and audio traffic on your network. Depending on the codecs used, audio streams consume from 21 kilobits per second (Kbps) (GMS 6.10 codec) to about 74.7 kilobits per second (Kbps) (G711). The video streams (aside from the codec) vary depending on the amount of movement in front of a camera. Expect 60 to 120 Kbps to be consumed by a video stream. There is a less than linear Kbps consumption increase corresponding to the number of attendees in a conference.

The H.323 clients send and receive a single video and a single audio stream from a video conference. Both multicast and H.323 clients can use Remote Access Services (RAS) to join video conferences over a dial up connection using 56 Kbps modems or Integrate Service Digital Network (ISDN). For multicast connectivity, the RAS server must run Windows 2000 Server, and Internet Group Management Protocol must be active.

Routers

If you have routers on your network and you want to use multicast conferencing across the router, you may have to configure your router to handle multicast packets. Use the MCAST diagnostic tool included with the Windows 2000 Resource Kit to determine which parts of your network are enabled for transmission of IP multicast packets. Use the tool in send mode to set up multicast sources at different locations on your network. Use it in

receive mode to determine where multicast traffic is being received. Windows 2000 also provides utilities to display the configuration of a multicast router (mrinfo), and to display multicast group tables and troubleshooting information for interfaces (routemon).

If your routers are not configured for multicast, you must create access lists specifying the range of multicast group addresses allowed to cross the router, and associate these lists with specific interfaces on different routers. For more information, see your Windows 2000 documentation.

Bridging Video Conferences

When a data and video conference resource is reserved for a conference, you can bridge the multicast video conference to H.323 NetMeeting clients. You can use the H.323 bridge for one of the following conditions:

- The client computer has Windows NT, or a Windows operating system earlier than Windows 2000 (not multicast enabled).
- The client browser does not support ActiveX controls.
- There is no multicast connectivity to the client computer.

When trying to join a conference, all clients check to see if they can establish a multicast connection to Conference Management Service by sending it a message. If a multicast connection can be established between Conference Management Service and the client, the client joins the multicast conference. If the client cannot connect to Conference Management Service, it connects to the MCU and the MCU requests an H.323 unicast call bridge to the multicast video conference. Figure 4.3 shows a Windows 98 client participating in a multicast conference using the H.323 bridge.

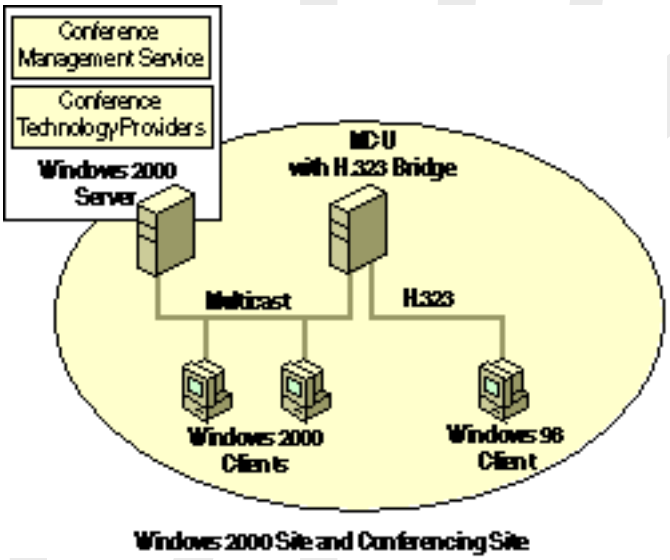

Figure 4.3 Bridging Video Conferences

For other multicast conference participants, this H.323 client looks and sounds like any other multicast participant. The H.323 client hears each participant in the conference, but receives only a single video image of thespeaking participant.

Because only a single video stream is sent to and from the H.323 client, even users with slow links are able to participate in video conferences.

To improve performance, you should install more than one MCU on the portion of your network where you have many simultaneous users. The MCUs in this area may have the same scope mask restricting client access to the specific subnets or none at all, because the site's Conference Management Service automatically balances the load among the MCUs.

To bridge video conferences, all MCUs that accept H.323 client connections must have multicast connectivity to the Conference Management Service on the server that is hosting the conference.

Resources

Video Conferencing Provider defines a resource size property based on the number of conference participants invited to online conferences at the same point in time. This maximum participant count defines the maximum number of audio and video streams that can be sent across the network at any point in time.

Each conference resource can also define the format of the video conference. You can configure the following properties on each Video Conferencing Provider conference resource:

- Whether the G.711 or GSM6.10 CODEC is used for transmitting audio,
- Whether video is enabled within the conference (audio-only conference).
- Whether the H.261 or H.263 CODEC is used for transmitting video.
- The size of the video image, QCIF or CIF.
- Is audio and/or video automatically sent for a participant when they first join a conference.
- Which Multicast scopes to use for the video conference.
- Whether H.323 bridging is permitted.

For a conference in which all participants are directly connected to the multicast video conference, Video Conferencing Provider monitors the conference and prevents too many participants from joining the conference.

Best Practices

When configuring IP address ranges for multicast scopes on your MADCAP server, there are two practices recommended by the Multicast Allocation working group, an IETF team of industry volunteers who help set multicast address allocation standards. These practices include:

Administrative scoping Use administrative scoping when you are using multicast IP addresses privately within your own network. You should start this scope in the **239.192.0.0** range. This range is known as the IPv4 Organization Local Scope and uses a subnet mask of 255.252.0.0 (14-bits in length).

> **Note** Administrative scoping is fully discussed in RFC 2365, "Administratively Scoped IP Multicast."

Global scoping Use global scoping when you are using multicast group IP addresses in a public network, such as the Internet.

Installation and Configuration

Installing Exchange Conferencing Server

This chapter describes the tasks you need to complete before you install Exchange Conferencing Server, as well as the tasks you need to complete after the installation.

Before the Installation

Before installing Exchange Conferencing Server, you need to plan your deployments and verify that you meet the system requirements for installing Exchange Conferencing Server.

Plan Your Deployment

Before proceeding with your deployment, review Chapter 3, *Planning Your Exchange Conferencing Server Installation* and Chapter 4, *Component Planning*. Use the information in these chapters to plan the structure of your conferencing site. Also, consider the following questions to help you design your implementation:

- How many Conference Management Services do you want to install?
- How many multipoint control units do you plan to install and where do you plan to install them?
- Do you want to support secure conferences?
- Do you need to bridge video clients?
- Where do you plan to install IIS?
- Do you want to accept connections from remote sites?
- Do you want to accept connections from the Internet?

Verify Requirements for Installation

Before installing Exchange Conferencing Server, verify that you meet the following system and hardware requirements. For additional information, review Chapter 4, *System Requirements* and *Hardware Requirements*.

System Requirements

You must install Exchange Conferencing Server on a Windows 2000 Server or Windows 2000 Advanced Server, and the following applications must be available in your organization:

- Microsoft Exchange 2000 Server
- Microsoft Windows 2000 MADCAP Services
- Microsoft Internet Information Services (IIS)
- Microsoft Windows 2000 Active Directory Service

- Microsoft Windows 2000 Certificate Services (only required if you plan to have secure conferences)

To take full advantage of the administrative functions in Conferencing Manager install it on the same server as Exchange System Manager.

> **Note** For an initial implementation, you can install all of these components on a single server. At a later time, you can deploy Exchange Conferencing Server to the rest of your organization.

Hardware Requirements

The following are the minimum required and minimum recommended hardware requirements for servers deploying Exchange Conferencing Server.

Minimum Required:

- 133 MHz Pentium processor
- 128 MB of RAM

Minimum Recommended:

- 400 MHz Pentium processor
- 256 MB of RAM

Installation

This section provides information about Exchange Conferencing Server components and procedures required for an initial installation and subsequent installations. With an initial installation, you might install all components. With subsequent installations, you might select individual components, such as the T.120 MCU/H.323 Conference Bridge to install on additional servers.

Conferencing Server Components

The following table describes the components listed on the Custom Setup screen in Exchange Conferencing Server Setup

Component	Function
Conference Management Service	Accepts reservations for online conferences, maintains conference schedules and controls conference technology providers. When you install this component Exchange Conferencing Server installs Data Conferencing Provider and Video Conferencing Provider
T.120 MCU/H.323 Conference Bridge	Provides a multipoint control unit for T.120 data conferencing clients and a bridge that allows H.323 clients to participate in audio and video conferences.

Conference Access Web Pages	A set of Web application pages hosted by IIS. Conference participants use these pages to participate in online conferences.
Conferencing Manager	A Microsoft Management Console tool for managing and configuring conferencing services.

Initial Installation

Use the following procedures to install a complete version of Exchange Conferencing Server, or to install only components that you select.

To install a complete version of Exchange Conferencing Server:

9. Log on to a Windows 2000 Server on which you want to install Exchange Conferencing Server. Insert the Exchange 2000 Conferencing Server CD into your CD-ROM drive.
10. On the **Welcome to the Installation Wizard for Microsoft Exchange 2000 Conferencing Server** screen, click **Next**.
11. On the **License Agreement** screen, read the license agreement. If you agree to the terms, click **I accept the terms of the license agreement**, and then click **Next**.
12. XXXXXXXXPlaceholder – **Product Identification** Screen??XXXXXXXXXXXX
13. On the **Setup Type** screen, click **Complete** to install all Exchange Conferencing Server components
14. XXXXXXXXPlaceholder – **Select Administrative Group** Screen??XXXXXXXXXXXX
15. On the **Ready to Install the Program** screen, click **Install**.

To install a custom version of Exchange Conferencing Server:

16. Log on to a Windows 2000 Server on which you want to install Exchange Conferencing Server. Insert the Exchange 2000 Conferencing Server CD into your CD-ROM drive.
17. On the **Welcome to the Installation Wizard for Microsoft Exchange 2000 Conferencing Server** screen, click **Next**.
18. On the **License Agreement** screen, read the license agreement. If you agree to the terms, click **I accept the terms of the license agreement**, and then click **Next**.
19. XXXXXXXXPlaceholder – **Product Identification** Screen??XXXXXXXXXXXX
20. On the **Setup Type** screen, click **Custom**, and then click **Next.**
21. On the **Custom Setup** screen, click the icon of each component and select your installation preference. Click **Change** if you want to change the install location.

    Note For information about available drives and their corresponding disk space, click **Space**.
22. XXXXXXXXPlaceholder – **Select Administrative Group** Screen??XXXXXXXXXXXX
23. On the **Ready to Install the Program** screen, click **Install**.

Subsequent Installation

After the initial installation of Exchange Conferencing Server, you can install additional copies of Exchange Conferencing components on other servers in your organization. For example, you can install additional copies of Conference Management Service and create additional multipoint control unit servers.

The procedure is the same as for a custom installation.

Post-Installation Tasks

After installing Exchange Conferencing Server, there are tasks you must perform on the server and on the client computers. This section outlines these tasks.

Server

After installing Exchange Conferencing Server, perform the following tasks to prepare your conferencing site for online conferences. For detailed procedures, see theExchange Conferencing Server online documentation.

- Create conference calendar mailbox
- Create conference resources

If you expect users on Exchange 5.5 servers to schedule online conferences, you need an Active Directory Connector (ADC) Connection Agreement to replicate conferencing resources from the Active Directory to the Exchange 5.5 directory. For detailed procedures on creating a Connection Agreement, see your Exchange online documentation.

Client

- After installing Exchange Conferencing Server, perform the following tasks to prepare your users to participate in online conferences. For detailed procedures, see the Exchange Conferencing Server online documentation. Allow Outlook 2000 users to directly reserve conference resources.
- Install ActiveX components on client computers that cannot download ActiveX controls.
- Provide certificates to your users for secure conferences.

DRAFT